DVTEL INC.
65 Challenger Road
Ridgefield Park, NJ 07660

Quasar CM-6204
Quasar CM-6208
Mini-Dome IP Camera
User and Installation Guide

The contents of this guide may not be reproduced or reprinted in whole or in part without the express written permission of DVTEL, Inc.

Rev. 02 March 12, 2015

Table of Contents

1 Document Information v

2 Overview 1

2.1 Features 2

2.2 Package Contents 3

3 Introduction to the CM-620x IP Mini-Dome Camera 5

3.1 Typical CM-6204 Camera 5

3.2 Camera Dimensions 5

3.3 Internal Connectors 6

3.4 System Cable Connectors 6

3.4.1 Waterproofing the Camera Cable Connectors 7

3.4.2 Connecting Power to the Camera 9

3.4.3 Input and Output Connectors 9

4 System Requirements 11

5 Installation 13

5.1 Indoor Installation 13

5.2 Outdoor Installation 13

5.3 Power and Ethernet Cable Connection 14

5.4 Initial Camera Configuration 14

5.5 Preparing the Camera for Use 15

5.6 Mounting Instructions 17

5.6.1 Mounting Tips 17

5.6.2 Mounting the Camera for Indoor or Outdoor Use 17

6 Using the DNA Utility to Search and Access the Camera 19

7 Configuring Communication Settings on the Quasar Camera 21

8 Adjusting and Framing-Up the Camera View 25

9 Configuration and Operation 27

9.1 Browser-Based Viewer Introduction 27

9.2 Live Screen 29

9.3 System Settings 31

9.3.1 System 31

9.3.2 Security 33

9.3.3 Network 42

9.3.4 Events Setup 52

9.3.5 Edge Recording 65

9.3.6 Motion Detection 71

9.3.7 Schedule 75

9.3.8 File Location 76

9.3.9 Maintenance 77
9.3.10 Import/Export 85
9.4 Streaming Settings 86
9.4.1 Video Format 86
9.4.2 Video Compression 96
9.4.3 Video ROI Encoding 98
9.4.4 Video OCX Protocol 99
9.4.5 Video Frame Rate 100
9.4.6 Video Mask 101
9.4.7 Audio 102
9.5 Camera Settings 103
9.5.1 Exposure 104
9.5.2 Picture Adjustment 109
9.5.3 Advanced Picture Settings 110
9.5.4 IR Function 114
9.5.5 Miscellaneous 116
9.6 Log Out 117
10 Appendices 119
A.1. CM-6204 Technical Specifications 120
A.2. CM-6208 Technical Specifications 123
A.3. Internet Security Settings 126
A.4. Install UPnP Components 128
A.5. Deleting the Existing DVPlayer 130
A.6. Deleting Temporary Internet Files 131
A.7. Mounting Accessories 132
Contacting DVTEL 134

List of Figures

Figure 1: Package Contents....3
Figure 2: Typical CM-6204 Series Camera with Motorized Lens....5
Figure 3: CM-6204 Series Camera Dimensions....5
Figure 4: MicroSDXC Card Drive and Reset Button....6
Figure 5: CM-6204 Camera Input/Output Connections....6
Figure 6: Camera Cables....7
Figure 7: System Cable....7
Figure 8: System Cable Hose and Wiring....8
Figure 9: RJ45 Connector and Plug....8
Figure 10: Thread-Lock Sealing Nut and RJ45 Connector....8
Figure 11: Loosened Thread-Lock Sealing Nut....8
Figure 12: RJ45 Connector and Thread-Lock Sealing Nut....9
Figure 13: Fastened Thread-Lock Sealing Nut....9
Figure 14: Discovered IP Devices....14
Figure 15: DNA Assign IP Dialog Box....15
Figure 16: Dome Cover....15
Figure 17: Exposed Mini-Dome Camera....16
Figure 18: Module-Fastening Screw....16
Figure 19: Rotated Lens Assembly....16
Figure 20: Base Plate Used as a Template to Mark Drilling Locations....17
Figure 21: Windows Firewall Screen....21
Figure 22: Discovered IP Devices....21
Figure 23: DNA Assign IP – Use DHCP Dialog Box....22
Figure 24: DNA Assign IP – Static IP Dialog Box....22
Figure 25: Installing the ActiveX Control....23
Figure 26: Security Window....23
Figure 27: Tilt-Arm Tension Screw on Tensioning Collar....25
Figure 28: CM-6204 Camera – Pan, Rotate and Tilt Angles....25
Figure 29: Browser-Based User Interface....27
Figure 30: Live View Screen....29
Figure 31: Live Video Info Dialog Box....29
Figure 32: System Section Tabs....31
Figure 33: System Screen....32
Figure 34: User Screen....33
Figure 35: Edit User Account Dialog Box....34
Figure 36: HTTPS Screen – Create Self-Signed Certificate....35
Figure 37: Create Self-Signed Certificate Dialog Box....36
Figure 38: Installed Certificate Section....36
Figure 39: Certificate Properties....37
Figure 40: HTTPS Screen – Upload Signed Certificate....37
Figure 41: HTTPS Screen – Install Signed Certificate....38
Figure 42: Create Certificate Request Dialog Box....38
Figure 43: Created Request Subject....39
Figure 44: Certificate Request Properties Dialog Box....39
Figure 45: IP Filter Screen....40
Figure 46: IEEE 802.1X/EAP-TLS Screen....41
Figure 47: Network > Basic Screen....42
Figure 48: QoS Screen....44
Figure 49: SNMP Settings Screen....45
Figure 50: UPnP Screen....47
Figure 51: Direct Access to Camera with UPnP Enabled....47
Figure 52: DDNS Screen....48
Figure 53: Mail Screen – SMTP....49
Figure 54: FTP Screen....50
Figure 55: HTTP Screen....51
Figure 56: IO Screen....52
Figure 53: Upload Image by FTP....53
Figure 54: Send HTTP Notification....54
Figure 55: Record Video Clip....54

Figure 56: Upload Image by E-Mail 54
Figure 61: Network Failure Detection Screen 56
Figure 62: Tampering Screen 57
Figure 63: Day/Night Trigger Screen 60
Figure 64: Periodic Event Screen 61
Figure 65: Manual Trigger Screen 63
Figure 66: SD Card Screen 65
Figure 67: Video File Recording List 66
Figure 68: Selected File Window 67
Figure 69: Network Share Screen 67
Figure 70: Video File Recording List 68
Figure 71: Selected File Window 69
Figure 72: Recording Screen 70
Figure 73: Motion Detection Screen 71
Figure 74: Motion Detection Screen – with Schedule Drop-Down Menu 72
Figure 75: Motion Window without Detection 72
Figure 76: Motion Window with Detection 73
Figure 77: Pixel Interval Illustration 73
Figure 78: Schedule Screen 75
Figure 79: File Location Screen 76
Figure 80: Log File Screen 77
Figure 81: User Information Screen – Get User Information 78
Figure 82: User Information – Get User Privacy 79
Figure 83: Factory Default Screen 80
Figure 84: Partial Restore Screen 81
Figure 85: Software Version Screen 82
Figure 86: Upgrade Screen 82
Figure 87: Software Upgrade – In Process 83
Figure 88: Parameter Screen 84
Figure 89: Import/Export Screen 85
Figure 90: File Download Screen 85
Figure 91: Streaming Section Tabs 86
Figure 92: CM-6204 Video Format Screen 87
Figure 89: CM-6208 Video Format Screen 88
Figure 93: View-1 (Source) 94
Figure 94: View-2 Image Rotated Vertically (Reversed) 94
Figure 95: CM-6204 Video Compression Screen 96
Figure 93: Video Compression Screen 97
Figure 96: Video ROI Encoding Screen 98
Figure 97: Video OCX Protocol Screen 99
Figure 98: Video Frame Rate Screen 100
Figure 99: Mask Screen 101
Figure 100: Audio Screen 102
Figure 101: Camera Section Tabs 103
Figure 103: CM-6204 Exposure Screen 105
Figure 104: Camera Settings Screen – Picture Adjustment 109
Figure 105: Advanced Picture Settings Screen – White Balance 110
Figure 106: Advanced Picture Settings Screen – Backlight 111
Figure 107: Advanced Picture Settings Screen – WDR Function 112
Figure 108: Advanced Picture Settings Screen – Noise Reduction 113
Figure 109: IR Function Screen 114
Figure 110: Camera Settings Screen – Digital Zoom 116
Figure 111: Login Message 117
Figure 112: Login Window 117
Figure 113: Command Bar Toolbar – Select Internet Options 126
Figure 114: Internet Options Screen 126
Figure 115: Command Bar Toolbar – Internet Options 127
Figure 116: Schedule Screen 127

1 Document Information

Document Conventions	*Conventions relatives au document*
WARNING and **CAUTION** notes are distributed throughout this document, whenever applicable, to alert you of potentially hazardous situations. These may be hazards associated with a task or a procedure you are carrying out or are about to carry out. The following document conventions are used throughout this manual:	*Les remarques **AVERTISSEMENT** et **ATTENTION** sont réparties dans l'ensemble du document, en fonction des besoins, afin de vous avertir des situations potentiellement dangereuses. Il peut s'agir de risques associés à une tâche ou à une procédure que vous effectuez ou êtes sur le point d'effectuer.* *Les conventions suivantes sont utilisées dans l'ensemble du document:*

A **Warning** is a precautionary message that indicates a procedure or condition where there are potential hazards of personal injury or death.

***Avertissement** est un message préventif indiquant qu'une procédure ou condition présente un risque potentiel de blessure ou de mort.*

A **Caution** is a precautionary message that indicates a procedure or condition where there are potential hazards of permanent damage to the equipment and or loss of data.

***Attention** est un message préventif indiquant qu'une procédure ou condition présente un risque potentiel de dommages permanents pour l'équipement et/ou de perte de données.*

A **Note** is useful information to prevent problems, help with successful installation, or to provide additional understanding of the products and installation.

*Une **Remarque** est une information utile permettant d'éviter certains problèmes, d'effectuer une installation correcte ou de mieux comprendre les produits et l'installation.*

A **Tip** is information and best practices that are useful or provide some benefit for installation and use of DVTEL products.

*Un **Conseil** correspond à une information et aux bonnes pratiques utiles ou apportant un avantage supplémentaire pour l'installation et l'utilisation des produits DVTEL.*

Document Scope and Purpose

The purpose of this document is to provide instructions and installation procedures for physically connecting the Quasar Gen II camera. After completing the physical installation, additional setup and configurations may be required before video analysis and detection can commence.

Note:
This document is intended for use by technical users who have a basic understanding of CCTV camera/video equipment and LAN/WAN network connections.

Remarque:
Ce document est destiné aux utilisateurs techniciens qui possèdent des connaissances de base des équipements vidéo/caméras de télésurveillance et des connexions aux réseaux LAN/WAN.

Warning:
Installation must follow safety, standards, and electrical codes as well as the laws that apply where the units are being installed.

Avertissement:
L'installation doit respecter les consignes de sécurité, les normes et les codes électriques, ainsi que la législation en vigueur sur le lieu d'implantation des unités.

Proprietary Rights and Non-Disclosure

This manual is delivered subject to the following restrictions and conditions:

- This document contains proprietary information belonging to DVTEL, Inc. This information is supplied solely for the purpose of assisting explicitly the licensee of the DVTEL units.
- No part of this document contents may be used for any other purpose, disclosed to any third party or reproduced by any means, electronic or mechanical, without the express prior written permission of DVTEL, Inc.

Trademarks and Copyrights

DVTEL, the DVTEL logo, Quasar Gen II, CM-6204, and Latitude are trademarks of DVTEL, Inc. Products and trademarks mentioned herein are for identification purposes only and may be registered trademarks of their respective companies. DVTEL, Inc. makes no representations whatsoever about any other products or trademarks mentioned in the manual.

This manual and its contents herein are owned by DVTEL, Inc. © DVTEL, Inc. 2015. All rights reserved.

Disclaimer	*Avis de non-responsabilité*
Users of DVTEL products accept full responsibility for ensuring the suitability and considering the role of the product detection capabilities and their limitation as they apply to their unique site requirements. DVTEL, Inc. and its agents make no guarantees or warranties to the suitability for the users' intended use. DVTEL, Inc. accepts no responsibility for improper use or incomplete security and safety measures. Failure in part or in whole of the installer, owner, or user in any way to follow the prescribed procedures or to heed WARNINGS and CAUTIONS shall absolve DVTEL, Inc. and its agents from any resulting liability. Specifications and information in this guide are subject to change without notice.	*Il incombe aux utilisateurs des produits DVTEL de vérifier que ces produits sont adaptés et d'étudier le rôle des capacités et limites de détection du produit appliqués aux exigences uniques de leur site.* *DVTEL, Inc. et ses agents ne garantissent d'aucune façon que les produits sont adaptés à l'usage auquel l'utilisateur les destine. DVTEL, Inc. ne pourra être tenu pour responsable en cas de mauvaise utilisation ou de mise en place de mesures de sécurité insuffisantes.* *Le non respect de tout ou partie des procédures recommandées ou des messages d'AVERTISSEMENT ou d'ATTENTION de la part de l'installateur, du propriétaire ou de l'utilisateur dégagera DVTEL, Inc. et ses agents de toute responsabilité en résultant.* *Les spécifications et informations contenues dans ce guide sont sujettes à modification sans préavis.*

Document Conventions	*Conventions relatives au document*
WARNING and **CAUTION** notes are distributed throughout this document, whenever applicable, to alert you of potentially hazardous situations. These may be hazards associated with a task or a procedure you are carrying out or are about to carry out. The following document conventions are used throughout this manual:	*Les remarques **AVERTISSEMENT** et **ATTENTION** sont réparties dans l'ensemble du document, en fonction des besoins, afin de vous avertir des situations potentiellement dangereuses. Il peut s'agir de risques associés à une tâche ou à une procédure que vous effectuez ou êtes sur le point d'effectuer.* *Les conventions suivantes sont utilisées dans l'ensemble du document:*

General Cautions and Warnings

This section contains information that indicates a procedure or condition where there are potential hazards. These may be hazards associated with a task or procedure a user is carrying out or about to carry out. WARNINGS and CAUTIONS are distributed throughout this document, whenever applicable, to alert the user of potentially hazardous situations.

SAVE ALL SAFETY AND OPERATING INSTRUCTIONS FOR FUTURE USE.

Although the unit is designed and manufactured in compliance with all applicable safety standards, certain hazards are present during the installation of this equipment.

To help ensure safety and to help reduce risk of injury or damage, observe the following:

Précautions et avertissements d'ordre général

Cette section contient des informations indiquant qu'une procédure ou condition présente des risques potentiels. Il peut s'agir de risques associés à une tâche ou à une procédure qu'un utilisateur effectue ou est sur le point d'effectuer. Les notes AVERTISSEMENT et ATTENTION sont réparties dans l'ensemble du document, en fonction des besoins, afin d'avertir l'utilisateur des situations potentiellement dangereuses.

***CONSERVEZ TOUTES LES INSTRUCTIONS DE SÉCURITÉ ET D'UTILISATION POUR POUVOIR VOUS Y RÉFÉRER ULTÉRIEUREMENT**.*

Bien que l'unité soit conçue et fabriquée conformément à toutes les normes de sécurité en vigueur, l'installation de cet équipement présente certains risques.

Afin de garantir la sécurité et de réduire les risques de blessure ou de dommages, veuillez respecter les consignes suivantes:

Warning:

1. The camera covers is an essential part of the product. Do not open or remove it.
2. Never operate the camera without the cover in place. Operating the camera without the cover poses a risk of fire and shock hazards.
3. Do not disassemble the camera or remove screws. There are no user serviceable parts inside the unit.
4. Only qualified trained personnel should service and repair this equipment.
5. Observe local codes and laws and ensure that installation and operation are in accordance with fire, security and safety standards.

Avertissement:

1. *Les caches de la caméra sont une partie essentielle du produit. Ne les ouvrez et ne les retirez pas.*
2. *N'utilisez jamais la caméra sans que le cache soit en place. L'utilisation de la caméra sans cache présente un risque d'incendie et de choc électrique.*
3. *Ne démontez pas la caméra et ne retirez pas ses vis. Aucune pièce se trouvant à l'intérieur de l'unité ne nécessite un entretien par l'utilisateur.*
4. *Seul un technicien formé et qualifié est autorisé à entretenir et à réparer cet équipement.*
5. *Respectez les codes et réglementations locaux, et assurez-vous que l'installation et l'utilisation sont conformes aux normes contre l'incendie et de sécurité.*

Caution:
To avoid damage from overheating or unit failure, assure that there is sufficient temperature regulation to support the unit's requirements (cooling/heating). Operating temperature should be kept in the range specified for the product (0° to 50°C/32° to 122°F), with no more than 90% non-condensing humidity.

Attention:
Afin d'éviter tout dommage dû à une surchauffe ou toute panne de l'unité, assurez-vous que la régulation de température est suffisante pour répondre aux exigences de l'unité (refroidissement/chauffage). La température de fonctionnement doit être maintenue dans la plage de température spécifiée pour le produit (0° à 50°C/32° à 122°F), sans condensation d'humidité supérieur à 90%.

Electrical Safety Notice and Warnings

Warning:

1. Read the installation instructions before you connect the unit to a power source**.**
2. Electrical safety should always be observed. All electrical connections must be performed by a certified electrician.
3. Use the supplied power supply and protect against static electricity, ground faults and power surges.
4. The unit uses a three-wire power cord to make sure that the product is properly grounded when in use. This is a safety feature. If the intended power outlet does not support three prongs, one of which is a ground, contact an electrician to install the appropriate outlet. NEVER remove or otherwise attempt to bypass the ground pin of the power cord. Do not operate the unit in the absence of a suitably installed ground conductor**.**
5. If you use an extension cord with this system, make sure that the total ampere rating on the products plugged into the extension cord does not exceed the extension cord ampere rating.
6. To avoid possible shock hazards or damaging the unit, assure that the positive and negative of the power leads are properly connected to the terminal block connector before plugging it into the unit or turning on the power source.
7. In the following situations, the electric power should be turned off immediately and appropriate repairs, replacements or remedies should be taken if:
   - The power line is damaged, frayed or shows heavy wear.
   - The unit has been physically crushed or deformed.
   - The unit has been exposed to water.
   - The unit has been exposed to, or shows signs of damage from, fire, intense heat, heavy smoke, fumes, or vapors.
   - Electrical connections of the unit become abnormally hot or generate smoke.
   - The unit has been dropped, damaged or shows signs of loose internal parts.
   - The unit does not operate properly.

Avis et avertissements relatifs à la sécurité électrique

Avertissement:

1. *Lisez les instructions d'installation avant de brancher l'unité à une source d'alimentation électrique.*
2. *Les consignes de sécurité électrique doivent toujours être respectées. Toutes les connexions électriques doivent être effectuées par un électricien qualifié.*
3. *Utilisez l'alimentation fournie, et protégez l'unité contre l'électricité statique, les défauts de mise à la terre et les surtensions.*
4. *Si l'unité utilise un cordon d'alimentation à trois fils, assurez-vous que le produit est correctement mis à la terre du produit lors de son utilisation. Ne retirez JAMAIS, et ne tentez pas de contourner la broche de mise à la terre du cordon d'alimentation. N'utilisez pas l'unité en l'absence d'un conducteur de mise à la terre installé correctement.*
5. *Si vous utilisez une rallonge avec ce système, assurez-vous que l'ampérage total des produits branchés sur la rallonge ne dépasse pas l'ampérage nominal de celle-ci.*
6. *Pour éviter tout risque de choc électrique ou d'endommager l'unité, assurez-vous que les bornes plus et moins de l'alimentation sont correctement raccordées au connecteur du bloc de jonction avant de le brancher sur l'unité ou d'activer la source d'alimentation.*
7. *Dans les situations suivantes, l'alimentation électrique doit être coupée immédiatement, et les réparations, remplacements ou solutions suivants doivent être effectués si :*
   - *Le cordon d'alimentation ou la prise (le cas échéant) est endommagé, effiloché ou très usé.*
   - *L'unité a subi un choc ou a été déformée.*
   - *L'unité a été exposée à de l'eau.*
   - *L'unité a été exposée à, ou montre des signes de dégâts par le feu, une chaleur intense, une fumée épaisse, des émanations ou des vapeurs.*
   - *Les connexions électriques chauffent de façon anormale ou produisent de la fumée.*
   - *L'unité est tombée, a été endommagée, ou certaines pièces internes semblent détachées.*
   - *L'unité ne fonctionne pas correctement.*

Minimizing EMI and RFI	*Minimisation des IEM et des IRF*
When wires run for a significant distance in an electromagnetic field, electromagnetic interference (EMI) can occur. Strong EMI (e.g. lightning or radio transmitters) can destroy the units and can pose an electrical hazard by conducting power through lines and into the system. Poor quality or worn wiring can result in radio frequency interference (RFI). To minimize the effects of EMI and RFI, consult your reseller.	*Lorsque des câbles parcourent une distance importante dans un champ électromagnétique, des interférences électromagnétiques (IEM) peuvent se produire. D'importantes IEM (comme la foudre ou un émetteur radio) peuvent détruire les unités et présenter un risque électrique si elles se propagent sur les câbles et dans le système. Des câbles de mauvaise qualité ou usés peuvent provoquer des interférences radioélectriques (IRF). Pour minimiser les effets des IEM et des IRF, consultez votre revendeur.*

Site Preparation

There are several requirements that should be properly addressed prior to installation at the site. The following specifications are requirements for proper installation and operation of the unit:

- **Ambient Environment Conditions**: Avoid positioning the unit near heaters or heating system outputs. Use proper maintenance to ensure that the unit is free from exposure to EMI.
- **Accessibility**: The location used should allow easy access to unit connections and cables.
- **Safety**: Cables and electrical cords should be routed in a manner that prevents safety hazards, such as from tripping, wire fraying, overheating, etc. Ensure that nothing rests on the unit's cables or power cords.
- **Ample Air Circulation**: Leave enough space around the unit to allow free air circulation.
- **Cabling Considerations**: Units should be placed in locations that are optimal for the type of video cabling used between the unit and the cameras and external devices. Using a cable longer than the manufacturer's specifications for optimal video signal may result in degradation of color and video parameters.
- **Physical Security**: The unit provides threat detection for physical security systems. In order to ensure that the unit cannot be disabled or tampered with, the system should be installed with security measures regarding physical access by trusted and un-trusted parties.
- **Network Security**: The unit transmits over IP to security personnel for video surveillance. Proper network security measures should be in place to assure networks remain operating and free from malicious interference. The unit is intended for installation on the backbone of a trusted network.
- **Electrostatic Safeguards**: The unit as well as other equipment connected to it (relay outputs, alarm inputs, racks, carpeting, etc.) shall be properly grounded to prevent electrostatic discharge.

The physical installation of the unit is the first phase of making the unit operational in a security plan. The goal is to physically place the unit, connect it to other devices in the system, and to establish network connectivity.

2 Overview

The DVTEL Quasar Gen II CM-620x series consists of two camera families: CM-6204 and CM-6208.

The Quasar CM-6204 is an indoor/outdoor, vandal-proof, IP mini-dome camera. The camera provides real-time, QHD H.264 multi-streaming with the highest quality image. It supports three simultaneous video streams at QHD 1440p, HD 720p, and D1 resolutions. The family consists of two cameras with a varifocal, motorized, auto-focus, P-Iris lens with True Day/Night and infrared IR illuminator:

- CM-6204-11-I includes a 3-8mm, F1.4 lens with 96-38° horizontal viewing angle
- CM-6204-21-I includes a 7-22mm, F1.4 lens with 42-14° horizontal viewing angle

The Quasar CM-6208 is an indoor/outdoor, vandal-proof, IP mini-dome camera. The camera provides real-time, 4K, H.264 multi-streaming with the highest quality image. It supports four simultaneous video streams at UHD 4K, Full HD 1080p, HD 720p, and D1 resolutions. The family consists of two cameras with a varifocal, motorized, auto-focus, F1.4, P-Iris lens with True Day/Night and infrared IR illuminator:

- CM-6208-11-I includes a 3.5-8mm lens with 116-50° horizontal viewing angle
- CM-6208-21-I includes a 9-22mm lens with 45-18° horizontal viewing angle

Caution:
If you are using DVTEL Latitude, we recommend that you configure the camera's settings via the AdminCenter. This is because the camera's web-based interface might be overwritten by Latitude settings. Refer to the Latitude online help for information regarding configuring camera settings.

Attention:
Si vous utilisez DVTEL Latitude, nous vous conseillons de configurer les paramètres de la caméra via l'AdminCenter. En effet, l'interface Internet de la caméra peut être remplacée par les paramètres Latitude. Veuillez consulter l'aide en ligne Latitude pour de plus amples informations sur la configuration des paramètres de la caméra.

2.1 Features

- H.264 and MJPEG compression
- HTTP streaming MJPEG
- Progressive scan CMOS sensor
- Edge motion detection
- Motion detection with region of interest masking
- Historical motion detection levels detected/recorded at frame levels
- Detection event driven alarms
- Alarm input driven events
- Relay output actions on alarm
- Built-in web application/web server
- FTP upload (up to two locations)
- Upload alarm images to FTP
- Dual HTTP notification server support (up to two servers)
- Send images on alarm to e-mail
- E-mail SMTP alarm notification (up to two e-mails)
- 128GB microSDXC recording support
- Record snapshots to microSDXC card on alarm
- Sequential snapshot numbering
- SNMP v1/v2/v3 and SNMP traps
- Security IP restricted access allow/deny list
- UPnP support
- Electronic day/night (ICR)
- Analog video output
- BNC analog output
- Privacy masks
- WDR and ATW
- 3DNR image noise reduction
- ONVIF support
- RTSP support
- Supports PoE/12VDC/24VAC
- Multiple users
- Group permissions
- Per-user permissions
- Tampering detection and notification
- Two encoder streams available
- Low-lux mode and backlight compensation
- Vandal-proof IP66 enclosure
- Motorized lens
- Infrared LED illuminator

2.2 Package Contents

Before proceeding, please check that the box contains the items listed here. If any item is missing or has defects, do not install or operate the product and contact your dealer for assistance.

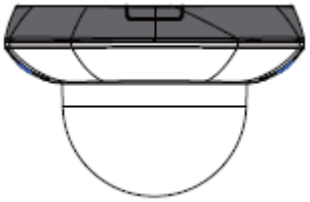
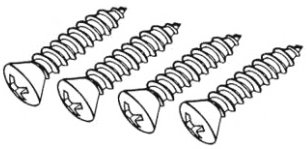
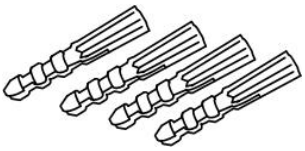
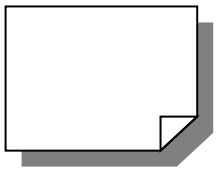
 Mini-dome camera	(Torx wrench)	Rubber washers (×6)
 Self-tapping screws (×4) (See note below)	 Plastic screw anchors (×4)	CD (Bundled software and documentation)
	 Quick Installation Guide	

Figure 1: Package Contents

Note:
The self-tapping screws are mainly for softer substrate/material installation such as wood. For other installation materials such as cement ceilings, it is necessary to pre-drill and use plastic anchors before fastening the supplied self-tapping screws into the wall.

Related Documentation

- *CM-620x Mini-Dome Camera Quick Installation Guide*
- *DNA 2.0 User Manual*

3 Introduction to the CM-620x IP Mini-Dome Camera

This chapter provides information about the camera hardware for reference before installation. The connectors included on the camera's system cable are described.

- Typical CM-6204 Camera
- Camera Dimensions
- Internal Connectors
- System Cable Connectors

3.1 Typical CM-6204 Camera

The figure below shows a typical CM-620x camera.

Figure 2: Typical CM-6204 Series Camera with Motorized Lens

3.2 Camera Dimensions

The CM-620x series indoor/outdoor vandal-proof motorized IP mini-dome camera dimensions are shown below.

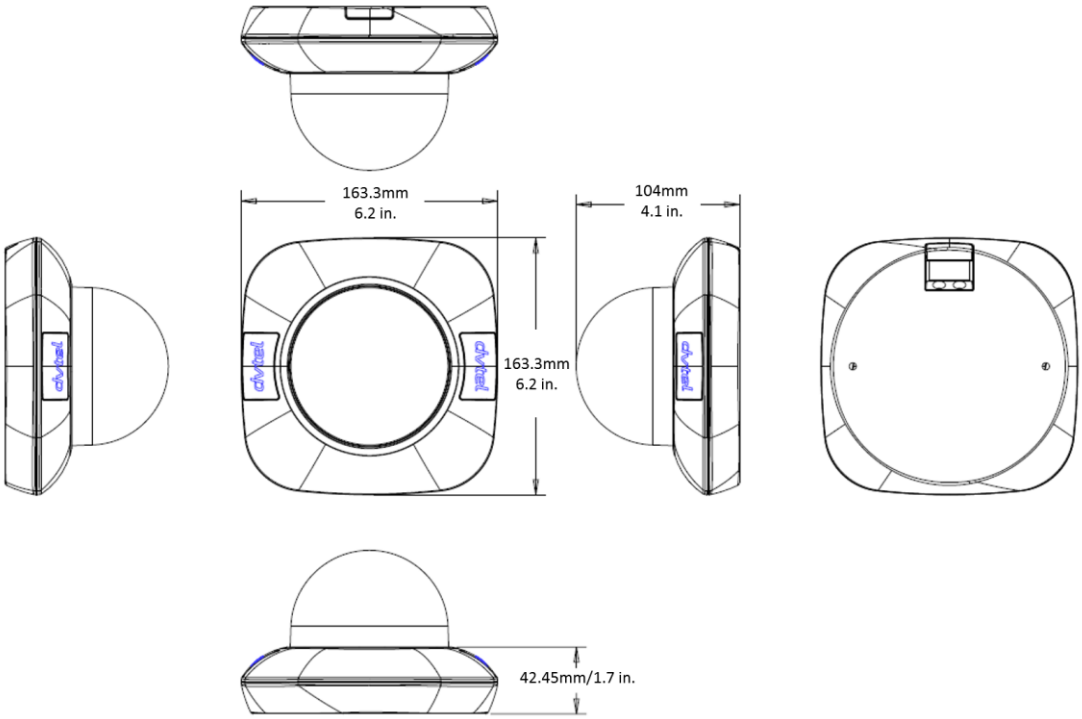


Figure 3: CM-6204 Series Camera Dimensions

3.3 Internal Connectors

As seen in the illustration below, the baseplate of the camera includes a microSDXC card drive, which can store up to 128GB of data. The base of the lens assembly includes a reset button.

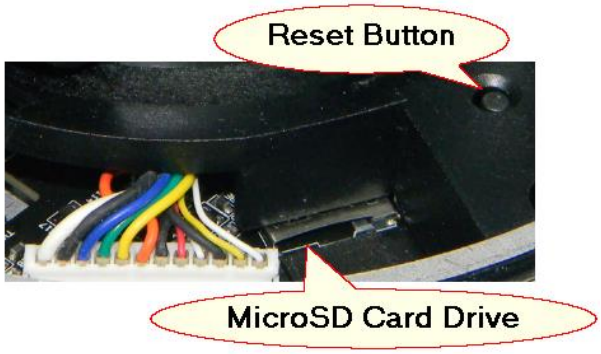


Figure 4: MicroSDXC Card Drive and Reset Button

To perform a hard reset to full factory defaults using the Reset button

1. Insert a pointed object into the Reset button.
2. Press the button for 30 seconds. Both LEDs on the RJ45 connector are extinguished. After one second, the green network LED flashes once and then remains lighted. The yellow activity LED flashes as soon as it detects network activity.
3. The unit returns to full factory defaults.

3.4 System Cable Connectors

The camera is shipped with a system cable for network, power, I/O, and audio connections. The figure below shows the various connectors included in the system cable of the camera. The connectors, pin numbers and signal definitions are listed below.

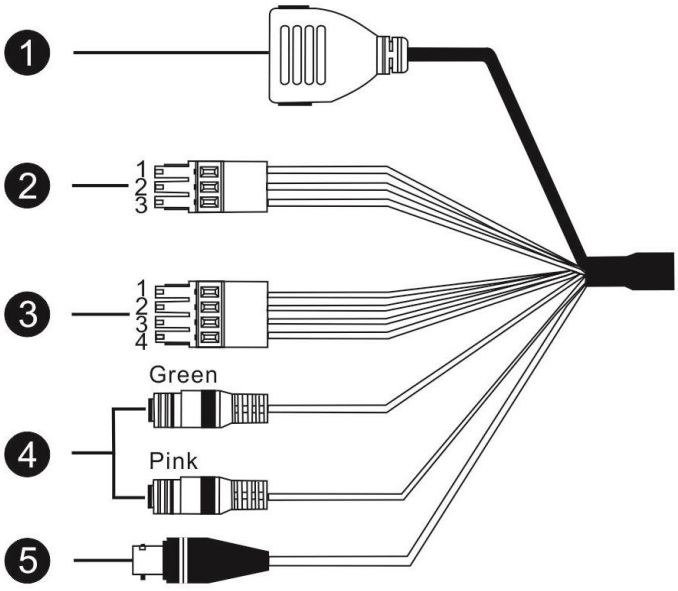


Figure 5: CM-6204 Camera Input/Output Connections

No.	Cable	Pin	Definition		Remarks
1	RJ45	-	For network and PoE connections		
2	Power (DC 12V*/AC 24V) (3-pin Terminal Block)	1	DC 12V −	AC 24V 1	Power connection
		2	Reserved	GND	
		3	DC 12V +	AC 24V 2	
3	Alarm I/O (4-pin Terminal Block)	1	Alarm In −		Alarm connection
		2	Alarm In +		
		3	Alarm Out −		
		4	Alarm Out +		
4	Audio I/O	Green	Audio Out		Two-way audio transmission
		Pink	Audio-in/Mic-in		
5	BNC	-	For analog video output		

3.4.1 Waterproofing the Camera Cable Connectors

Follow the instructions below to waterproof the connectors for the different types of cables included in the system cable. The cables are shown below.

System Cable **RJ45 Cable** **IP66 RJ45 Cable**

Figure 6: Camera Cables

3.4.1.1 System Cable

To waterproof the system cable

1. Connect all the required devices to the system cable.
2. Coat the joints with silicone gel. There should be no gap between the connectors and the cables. For alarm I/O connector and power connector, make sure the side with wires attached is also sealed with silicone gel.

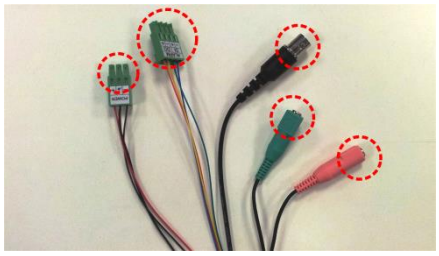


Figure 7: System Cable

3. Seal the end of the rubber coating of the system cable as indicated in the figure below. Use enough silicone gel to fill in the hose and wrap around each wire in order to properly waterproof the cable.

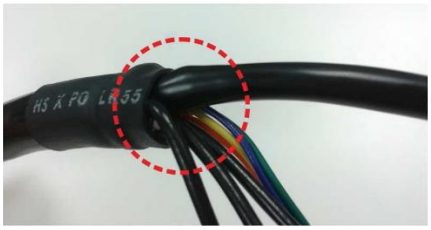


Figure 8: System Cable Hose and Wiring

3.4.1.2 RJ45 Cable

To waterproof the RJ45 cable

1. Plug the Ethernet cable to the connector of the RJ45 cable.

Figure 9: RJ45 Connector and Plug

2. Coat the joint with silicone gel. Make sure there is no gap between the Ethernet cable and the connector in order to properly waterproof the cable.

3.4.1.3 IP66-Rated RJ45 Cable

To waterproof the IP66-Rated RJ45 cable

1. Remove the supplied connector from the IP66-rated RJ45 plug.

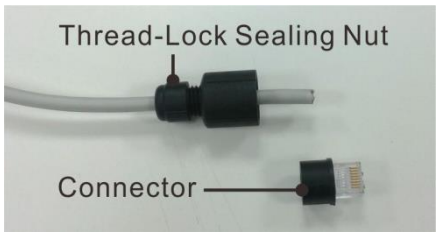


Figure 10: Thread-Lock Sealing Nut and RJ45 Connector

2. Loosen the thread-lock sealing nut on the IP66-rated RJ45 plug.

Figure 11: Loosened Thread-Lock Sealing Nut

3. Thread the Ethernet cable through the thread-lock sealing nut and the IP66-rated RJ45 plug. If the Ethernet cable is already attached to a connector, remove it first.

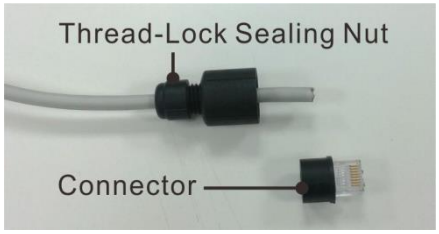


Figure 12: RJ45 Connector and Thread-Lock Sealing Nut

4. Carefully remove a section of rubber coating from the end of the Ethernet cable to reveal the wires.
5. Inset the wires into the correct pins of the connector.
6. Plug the Ethernet cable into the connector of the IP66-rated RJ45 cable.
7. Fasten the RJ45 plug to the connector of the IP66-rated RJ45 cable.
8. Tighten the thread-lock sealing nut to the plug.

Figure 13: Fastened Thread-Lock Sealing Nut

3.4.2 Connecting Power to the Camera

The camera can be powered by Power over Ethernet or by an external 12VDC/24VAC adaptor (not included in the package).

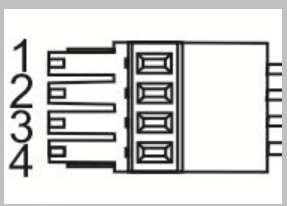
- If using an external power supply, connect the power leads or three-pin power terminal block to the power supply.
- If using PoE, make sure that a Power Sourcing Equipment (PSE) device is used in the network

Make sure the camera's power cable is properly connected. All electrical work must be performed in accordance with local regulatory requirements.

3.4.3 Input and Output Connectors

The alarm input and output connectors are shown below.

Pin No.	Designation
1	Input (-)
2	Input (+)
3	Output (-)
4	Output (+)



4 System Requirements

To access the camera via a web browser, ensure that your PC has the proper network connection and meets system requirements as described below.

Item	Minimum System Requirement
Personal Computer	Minimum: Intel® Core™ i5-2430M @ 2.4 GHz, 4GB RAM Recommended: Intel® Core™ i7-870 @ 2.93 GHz, 8GB RAM
Operating System	Windows XP, Windows 7, Windows 8, Windows 8.1
Web Browser	Microsoft Internet Explorer 9, 10, or 11
Network Card	10BaseT (10 Mbps), 100Base-TX (100 Mbps), or 1000BaseT (1000Mbps) operation
Viewer	ActiveX control plug-in for Microsoft IE

5 Installation

Follow the instructions below for indoor and outdoor installation of the camera.

Related Links

- Indoor Installation
- Outdoor Installation
- Power and Ethernet Cable Connection
- Initial Camera Configuration
- Preparing the Camera for Use
- Mounting Instructions

5.1 Indoor Installation

Read the instructions provided in this chapter thoroughly before installing the camera. Following are additional considerations for indoor installation:

- There must be a fuse or circuit breaker at the starting point of the electrical wiring infrastructure.
- For indoor installations, such as industrial applications, the camera must be protected from hostile external elements (e.g. corrosive environment, metallic dust, extreme temperatures, soot, over spray, etc.).
- Do not place the camera on or near radiators and heat sources.
- All electrical work must be performed in accordance with local regulatory requirements.

5.2 Outdoor Installation

Read the instructions provided in this chapter thoroughly before installing the camera. Following are additional considerations for outdoor installation:

- For outside wiring installation, always use weatherproof equipment, such as boxes, receptacles, connectors, etc.
- For electrical wiring, use the properly rated sheathed cables for conditions to which the cable will be exposed (for example, moisture, heat, UV, physical requirements, etc.).
- Plan ahead to determine where to install infrastructure weatherproof equipment. Whenever possible, ground components to an outdoor ground.
- Use best security practices to design and maintain secured camera access, communications infrastructure, tamper-proof outdoor boxes, etc.
- All electrical work must be performed in accordance with local regulatory requirements.

5.3 Power and Ethernet Cable Connection

Make sure the camera's power cable is properly connected. Refer to System Cable Connectors. If using Power over Ethernet (PoE), make sure Power Sourcing Equipment (PSE) is available on the connected network. All electrical work must be performed in accordance with local regulatory requirements.

5.4 Initial Camera Configuration

To perform the initial camera configuration

1. Unpack the camera.
2. Connect one end of the network Cat 5 Ethernet cable to the RJ45 connector on the camera's system cable.
3. Connect the other end of the network cable to a Power Sourcing Equipment (PSE) device, such as a switch.
4. Verify that the LEDs on the RJ45 connector illuminate green (indicating a stable network connection) and flashing yellow (to indicate network activity).
5. Do the following:
   a. Copy and run `dna.exe` (see note below) from the included CD.

> **Note:**
> DNA is an enhanced software alternative to Device Search. Either of these programs may be used. They are supplied on the included CD.

   b. Click the icon.
   c. Select the unit requiring IP assignment.

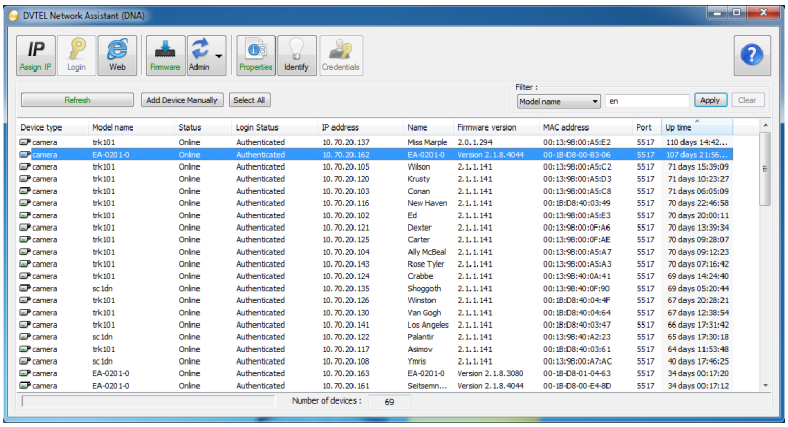


Figure 14: Discovered IP Devices

   d. Right-click the mouse and select the assigned IP address or click the **Assign IP** button to open the **DNA Assign IP** dialog box.

> **Note:**
> The camera default IP Address and the subnet mask IP Address are automatically supplied by the DHCP server.

   e. In the dialog box that is displayed, enter values for the *IP Address, Gateway and Netmask*.

f. Click **Update** and wait for ✔ *OK* status to be displayed.

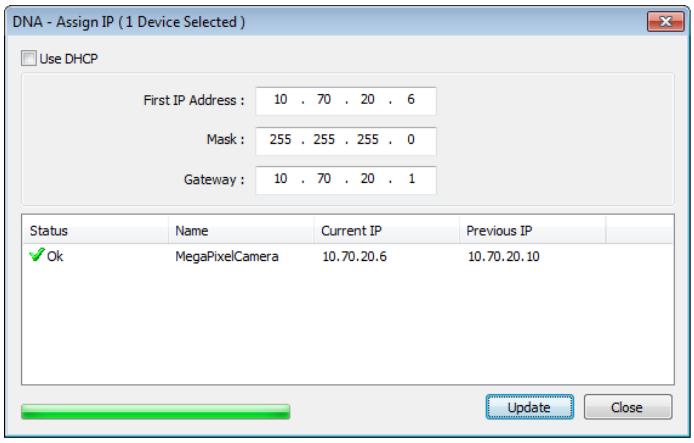


Figure 15: DNA Assign IP Dialog Box

g. Disconnect the Ethernet cable. The camera is ready for deployment (mounting) in a site installation.

Note:

1. The camera can be connected to a PC for bench installation via an Ethernet cross-cable.
2. The camera default IP Address is automatically set by the DHCP server. If using Latitude, the Address must be set manually.

Tip:
A camera setup adapter, such as Veracity Pinpoint, can be used to connect a laptop directly to the camera when using PoE.

5.5 Preparing the Camera for Use

Before using the camera, you must release the lens assembly, which is in a fixed position for shipping from the factory.

To release the lens assembly for use

1. Remove the mini-dome cover by opening the rubber tabs and unscrewing the screws located under the tabs with the star-bit tool supplied with the camera.

Figure 16: Dome Cover

2. Separate the top and bottom sections of the cover in order to access the camera module

Figure 17: Exposed Mini-Dome Camera

3. Unscrew the module-fastening screw sufficiently so that the lens assembly can rotate by 90°.

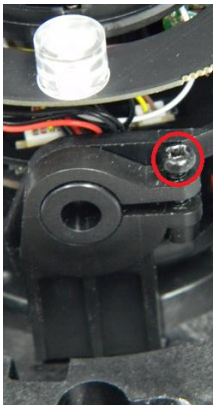


Figure 18: Module-Fastening Screw

4. Twist the lens assembly 90° in either direction in order to verify that the module can easily pan, tilt and rotate in any position.

Figure 19: Rotated Lens Assembly

5. Reinstall the dome cover, replace the screws, tighten them, and snap the rubber tabs back into position.

5.6 Mounting Instructions

The following are mounting instructions for the camera.

- Mounting Tips
- Mounting the Camera for Indoor or Outdoor Use

5.6.1 Mounting Tips

To eliminate IR reflection

1. Clean the bubble from dirt and finger prints.
2. Make sure the bubble has no scratches.
3. Fasten the screw that secures the snap-in chassis in order to have the rubber sealed against the bubble.
4. Avoid aiming the IR where there are nearby objects closer than the scene of interest which might reflect back into the lens.

5.6.2 Mounting the Camera for Indoor or Outdoor Use

1. Do one of the following:
   - For drilled wall or ceiling mounting:

     a) Using the supplied template, mark with a pointed pencil the mounting surface through the plate holes where the four screw holes need to be drilled. See Figure 20.

> **Note:**
> Before marking and drilling the holes, ensure that the base plate alignment is oriented correctly so that the required camera field of view can be achieved when the system is assembled.

Figure 20: Base Plate Used as a Template to Mark Drilling Locations

     b) In the marked locations, drill each hole using a drill bit of a slightly smaller diameter than the supplied screw anchors (molly-plug anchor). You want to achieve a snug insertion so that the plug expansion holds firm after the screws are screwed in.

     c) Fully insert the supplied anchors into drilled holes. You may need to tap them flush with the wall using a hammer.

- For installing on a 4S recessed electrical box:

  a) Have a qualified installer (check your local electrical codes) rough-in the 4S recessed electrical box and run the wires and power (if not PoE) through the wall/conduits to the box location.

  b) Ensure that the box is sufficiently sturdy (attach to the wall stud, ceiling joist, or reinforced surface as needed) to securely hold the weight of the camera.

- For bracket, pole and pendant installations:

  a) Thread the cables and any other wires (such as a relay output, alarm input, audio in, or audio out) through the mounting accessory.

Note:
The power cable is not required if using PoE.

Tip:
1. Even if you are not using alarm inputs and audio input/output at the time of installation, you may want to consider pre-wiring these connections for future use.
2. Use shims for shoring up mounts on uneven surfaces.

2. Thread the wires through the base plate and screw it to the pre-drilled wall, ceiling, CM Series Mini-Dome Recessed Mount, CM Series Mini-Dome Corner Mount, or 4S electrical box. Check that the installation is not flimsy, will not wobble, and is flush with the mounting surface.
3. Plug the Cat 5 cable into the camera's Ethernet port and, if needed, plug the power terminal block into the power terminals.
4. If applicable, wire the Alarm In, Alarm Out, Audio In, and Audio Out terminal blocks to external devices. See System Cable Connectors (page 6).
5. If needed, connect the other end of the Cat 5 cable to the network and turn on the power from the power supply.

Note:
Do not reassemble the camera's inner cover and mini-dome cover until after hardware configurations and lens adjustments are made.

6 Using the DNA Utility to Search and Access the Camera

The DVTEL Network Assistant (DNA) is a user-friendly utility that is designed to easily discover and configure DVTEL edge devices on a network. The DNA tool has a simple user interface and does not require any installation. The software is provided as a single, standalone executable. It runs on any PC.

DNA provides a central location for listing all the DVTEL camera models accessible over the network. Once listed, each camera can be right-clicked to access and change the network settings. If the network settings are changed for some reason, a new search will relist the units. The units may then be configured via the web interface.

If DVTEL Latitude is being used, configure the unit with a static IP address rather than with DHCP. This ensures that the IP address will not automatically change in the future and interfere with configurations and communication.

The camera must be made accessible for setting network addresses.

Note:
For detailed guidelines about DNA and its usage, refer to the *DNA 2.0 User Manual*, which is included in the CD provided with the camera.

7 Configuring Communication Settings on the Quasar Camera

To configure communication settings on the camera

1. Connect the camera to the network on the same VLAN/LAN as the workstation.
2. If the network supports the default, open the DNA utility by running `dna.exe` which can be found in the DNA Utility folder in the supplied CD, or click the DNA icon .

> **Note:**
> DNA is an alternative software to Device Search. Either of these programs may be used.

3. In the DNA application, click the **DNA** button.
4. If the Windows Firewall is enabled, a security alert window pops up.
5. To continue, click **Allow Access**. Latitude users should consult the Latitude Installation Instructions on disabling the Windows Firewall.

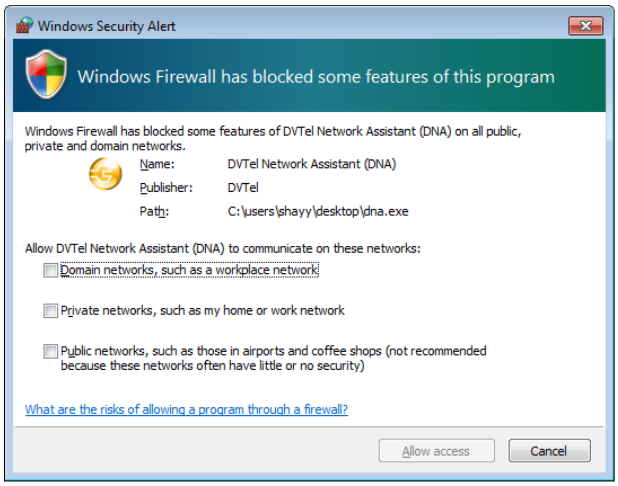

Windows Security Alert
Windows Firewall has blocked some features of this program
Windows Firewall has blocked some features of DVTel Network Assistant (DNA) on all public, private and domain networks.
Name: DVTel Network Assistant (DNA)
Publisher: DVTel
Path: C:\users\shayy\desktop\dna.exe
Allow DVTel Network Assistant (DNA) to communicate on these networks:
Domain networks, such as a workplace network
Private networks, such as my home or work network
Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security)
What are the risks of allowing a program through a firewall?
Allow access
Cancel

Figure 21: Windows Firewall Screen

6. Click **Assign IP**. All the discovered IP devices will be listed in the page, as shown in the figure below. The camera's default IP Address is automatically supplied by the DHCP server.

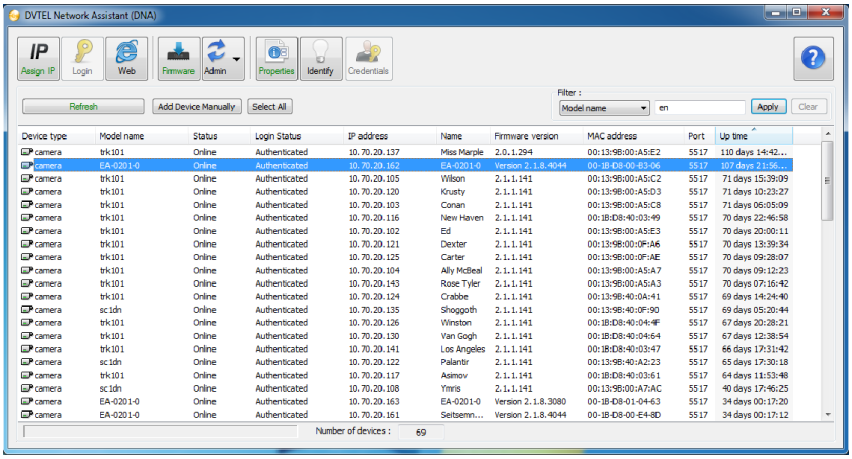


Figure 22: Discovered IP Devices

7. Right-click the camera whose network property is to be changed. From the context menu that opens, select **Assign IP**. The **Assign IP** dialog is displayed.

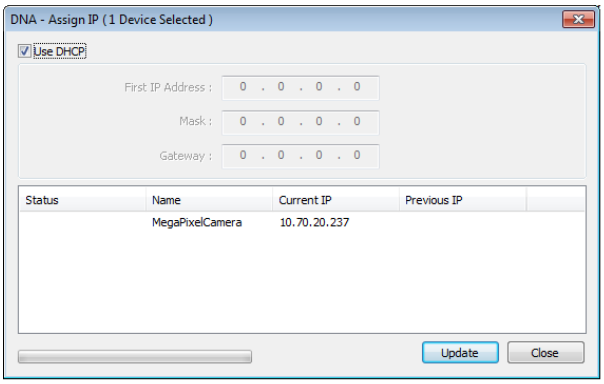


Figure 23: DNA Assign IP – Use DHCP Dialog Box

Tip:
Record the camera's MAC address for future reference.

8. To access DNA, do one of the following:
   a. For DHCP (not supported by Latitude):
      i. Select *Use DHCP*. Do not use for Latitude.
      ii. Click **Update** and wait for status.
   b. For Static IP (recommended for Latitude users):

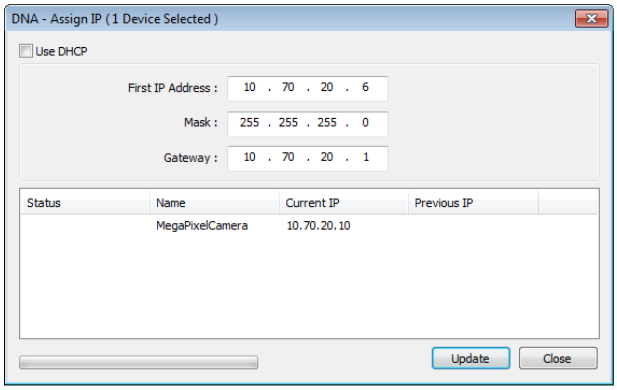


Figure 24: DNA Assign IP – Static IP Dialog Box

      i. Do not select the *Use DHCP* checkbox. This is recommended for security purposes and for and Latitude users. In the IP Address, Gateway, and Netmask, enter the respective LAN/VLAN (optional DNS) values.
      ii. Click **Update** and wait for *OK* status to be displayed.

9. Right-click and select **Web** to directly access the camera via a web browser. The default web browser opens and requests access to the camera IP address.

10. When the web browser contacts the camera IP, do the following:

    a. Login using the default user name *Admin* and password *1234***.**

> **Note:**
> User name and password are case-sensitive.

> **Note:**
> It is strongly advised that administrator's password be altered for security reasons.

    b. If the Information Bar (just below the URL bar) prompts for permission to install the ActiveX Control for displaying video in the browser (see the figure below), right-click the Information Bar. Select **Install ActiveX Control** to allow the installation.

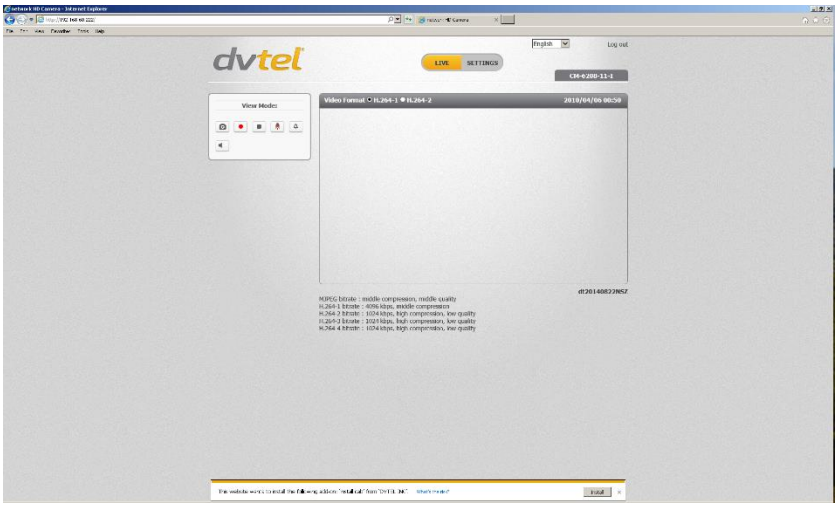


Figure 25: Installing the ActiveX Control

If a security warning window prompt appears, click **Install**.

Internet Explorer - Security Warning
Do you want to install this software?
Name: install.cab
Publisher: DVTEL INC
More options
Install
Don't Install
While files from the Internet can be useful, this file type can potentially harm your computer. Only install software from publishers you trust. What's the risk?

Figure 26: Security Window

11. If a popup message appears for running the DVPlayer add-on, click **Allow**.

> **Note:**
> If the password is changed and DVTEL Latitude AdminCenter Discovery feature is in use, deselect all other proprietary types. Select **DVTEL Quasar Gen II Series** so that the new password can be configured in the Discovery tab settings.

Additionally, you can change the camera's network properties (either DHCP or Static IP) directly from the camera's web interface on the System > Network > Basic screen.

8 Adjusting and Framing-Up the Camera View

After the camera is connected to the network and running, it is necessary to frame-up the scene and adjust the camera settings to optimize the picture for the individual scenes. If Latitude is being used, consider scheduling different settings for changing ambient conditions throughout the day, week, month or seasons.

To adjust and frame-up the camera view

1. In the DNA application, click **DNA**.
2. In the Discovery list, click to select the camera.
3. Right-click the context menu and select **Web**, or enter the camera's IP address in your browser's URL address bar.
4. When the browser connects to the camera and prompts for login, do the following:
   a) Log in using the default user name *Admin* and password *1234*. If the password has previously been changed, use the new password.

   Note:
   Both the user name and password are case sensitive.

   b) Allow the ActiveX to download and choose to install the DVTEL Web Player (DVPlayer).
   c) After the unit's web interface opens, use the function buttons on the Home page to adjust the zoom or focus.
5. If necessary, use a Phillips screwdriver to loosen the tilt-arm tension screw on the tensioning collar to adjust the camera tilt axis.

Figure 27: Tilt-Arm Tension Screw on Tensioning Collar

6. If necessary, adjust the rotation, pan and tilt angles as required for the desired view of the scene. When finished, retighten the tilt-arm tension screw.

Figure 28: CM-6204 Camera – Pan, Rotate and Tilt Angles

Caution:
To prevent camera damage, do not over extend the tilt range beyond -10° to 90°.

Avertissement:
Pour ne pas endommager la caméra, respectez une inclinaison comprise entre -10° et 90°.

Tip:
To view greater image detail for more accurate high-definition focusing, on the web-based Viewer home page, right-click the image, click **Full Screen**, and then check the focus.

Note:
Best focusing results can be achieved when the lens iris is fully open (such as at night in low light). This prevents loss of sharpness if light levels are reduced at night.

7. To achieve optimum focus results during daytime, open the **Camera > Exposure** screen in camera's web interface and select *Auto Shutter* mode. Save changes and complete the focusing steps. When finished, restore your exposure settings as needed.
8. Replace the camera's inner cover.
9. Replace the mini-dome cover and tighten the screw.

9 Configuration and Operation

The Quasar Gen II CM series camera is provided with a browser-based configuration interface for video playback and recording. In this chapter, information about main page introduction, system related settings and camera settings are described in detail.

Additionally, if DVTEL's Latitude VMS is used, many of the configurations and features of DVTEL's VMS provide configuration and automation of the camera.

This section includes the following information:

- Browser-Based Viewer Introduction
- Live Screen
- System Settings
- Streaming Settings
- Camera Settings
- Logout

9.1 Browser-Based Viewer Introduction

The figure below shows the Quasar Gen II CM-620x camera's browser-based user interface.

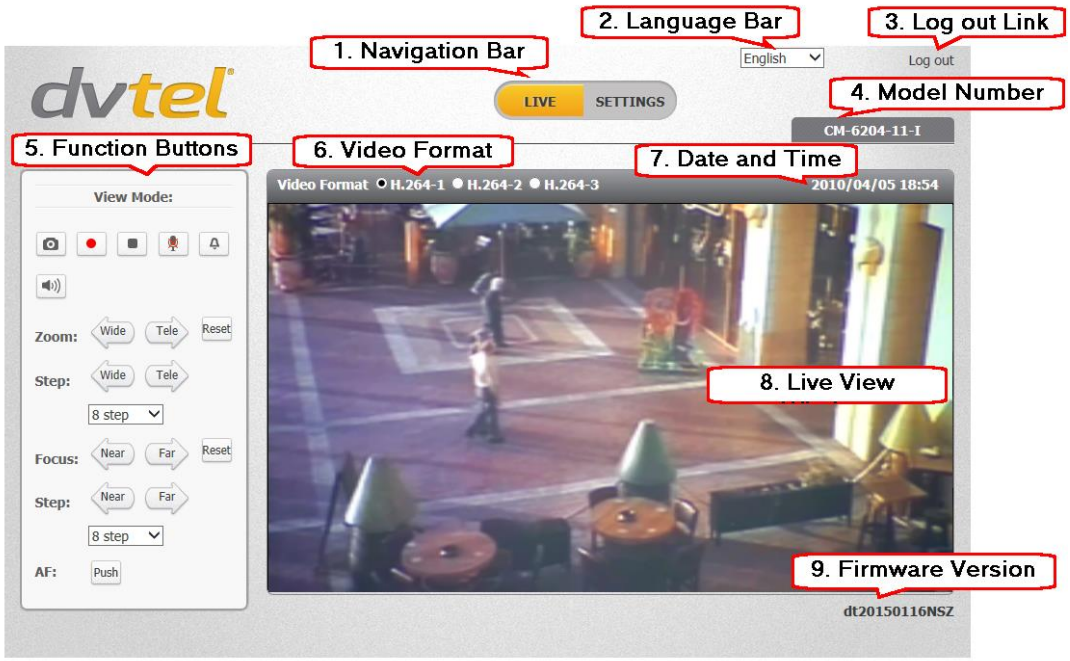


Figure 29: Browser-Based User Interface

The user interface displays the following information:

1. The Navigation Bar is displayed in the center of the screen containing **Live** and **Settings** buttons.
    - **Live Button**
      The **Live** screen opens by default when the camera logs on. It is used to monitor live video of the targeted area, adjust the display size, take snapshots of the view area, stop/start video streaming, record video in a designated file location, activate or de-activate a loudspeaker (audio function), and to perform a digital zoom. An explanation of the items on the screen is included below and in section 9.2.
    - **Settings Button**
      Clicking the **Settings** button opens the **Settings** screen, whose sidebar which includes three tabs – **System, Streaming,** and **Camera** – that are used for to configure system settings.
        - **System Settings**
          The administrator can configure settings for basic system parameters, security, network operation, events, recording, storage, system maintenance, and more. Details are discussed in System Settings.
        - **Streaming Settings**
          The administrator can modify video and audio settings on this page. Details are discussed in Streaming Settings.
        - **Camera Settings**
          The administrator can adjust many of the camera settings on this page, such as Exposure, Picture Adjustment, IR Function, Digital Zoom, and TV System. Details are discussed in Camera Settings.
2. The Language Bar is displayed to the right of the Navigation Bar. Supported languages include English, German, Spanish, French, Italian, Japanese, Korean, Portuguese, Russian, Simplified Chinese, and Traditional Chinese.
3. The *Log out* link is located to the right of the Language Bar. Click the *Log Out* link to exit the application or log into the camera with a different username and password. See Log Out.
4. The camera model number is displayed under the *Log out* link.
5. Function buttons are displayed to the left of the Live View window. These are discussed in the following section.
6. The video format is displayed and can be selected to the left of the date and time.
7. The current date and time are displayed under the model number.
8. In the center of the interface is the Live View window, which displays the image that the camera is monitoring.
9. The firmware version of the camera is displayed under the Live View window on the right side.

9.2 Live Screen

The camera's **Live** screen is used to monitor live video.

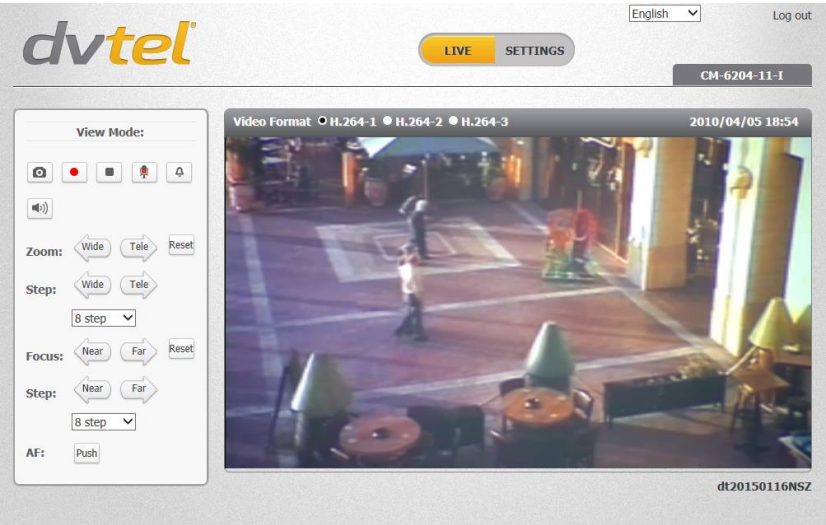


Figure 30: Live View Screen

Right-clicking the Live window opens the **Info** dialog box, which displays key details about the video stream:

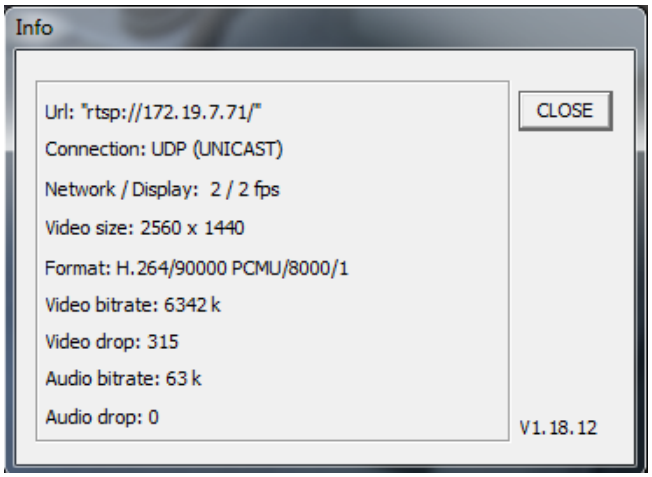


Figure 31: Live Video Info Dialog Box

The *View Mode* area in the **Live** screen includes the following function buttons:

Snapshot

Click this button to automatically save the JPEG snapshots in the specified location. The default location to save snapshots is: C:\.To change the storage location, refer to File Location.

Record/Pause

Pressing the **Recording** button stores recordings from the Live View in the location specified on the local hard drive, which can be configured in the **File Location** screen. The default storage location for the web recording is: C:/. Refer to File Location for details.

Video Streaming Restart/Stop

Press the **Stop** button to disable video streaming and to display the live video as black. Press **Restart** to show the live video again.

Mic

The **Microphone** button allows the local site to talk to the remote site. Click the button to switch it on/off. This function is available only to a user who has been granted this privilege by the Administrator. Refer to User in the Security section for further details.

Manual Trigger

This button enables you to trigger an action defined on the **System > Events Setup > IO** screen, which enables control over input and output alarms.

Speaker

Click the **Speaker** button to mute/activate the audio. This function is available only to a user who has been granted this privilege by the Administrator. Refer to User in the Security section for further details.

Zoom: Wide/Tele

Press the **Tele** or **Wide** button to implement continuous zoom adjustment.

Zoom Reset

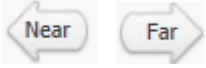
Press the **Rese**t button to calibrate the camera lens at full wide end.

Step: Wide/Tele

Press the **Wide Step** or **Tele Step** button to alternate the zoom between wide and telephoto views within a user-defined range of steps, which can be selected from the drop-down menu shown below.

Step Range

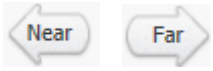
Select from a user-defined range of steps, which can be selected from the drop-down list.

Focus: Near/Far 

Press the **Near** or **Far** button to implement continuous focus adjustment.

Focus Reset

Press the **Rese**t button to calibrate the camera lens at infinity focus.

Step: Near/Far 

Press the **Near Step** or **Far Step** button to alternate the focus between near and far views within a user-defined range, which can be selected from the drop-down menu.

Step Range

Select from a user-defined range of steps, which can be selected from the drop-down list.

AF: Push

Click the **Push** button once to adjust zoom or focus. In this mode, the camera automatically and continuously maintains focus regardless of zoom or view changes. The focus status is displayed above the Live View pane.

9.3 System Settings

The **Settings** tab in the Navigation Bar opens the sections in the sidebar that are used for configuring the camera. Three sections are available for configuration**:** System, Streaming, and Camera.

9.3.1 System

The **System** section includes the following tabs:

- System
- Security
- Network
- Events Setup
- Edge Recording
- Motion Detection
- Schedule
- File Location
- Maintenance
- Import/Export

Note:
The **System** screen is accessible only by the Administrator.

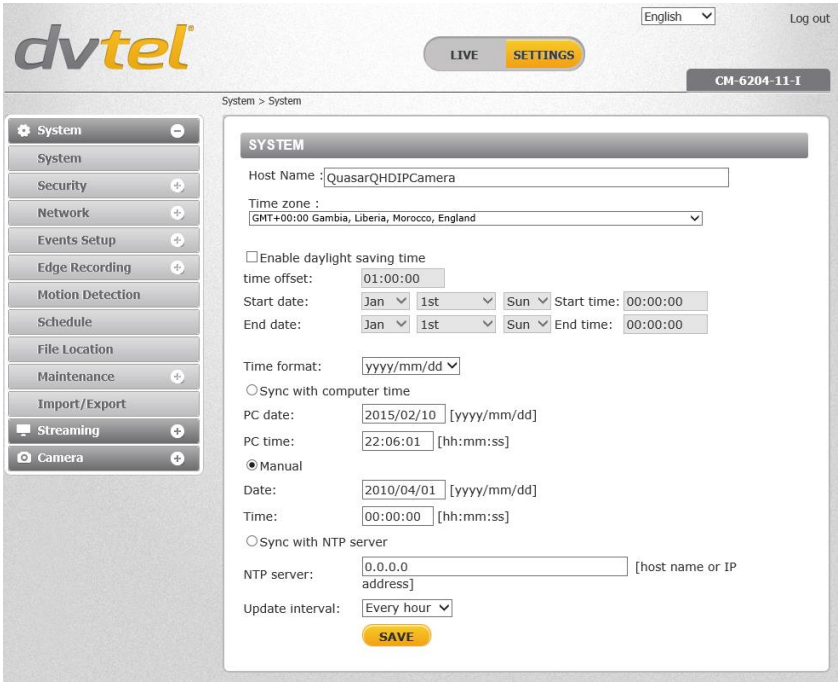


Figure 32: System Section Tabs

Click the **System** tab in the sidebar. The **System** screen is displayed.

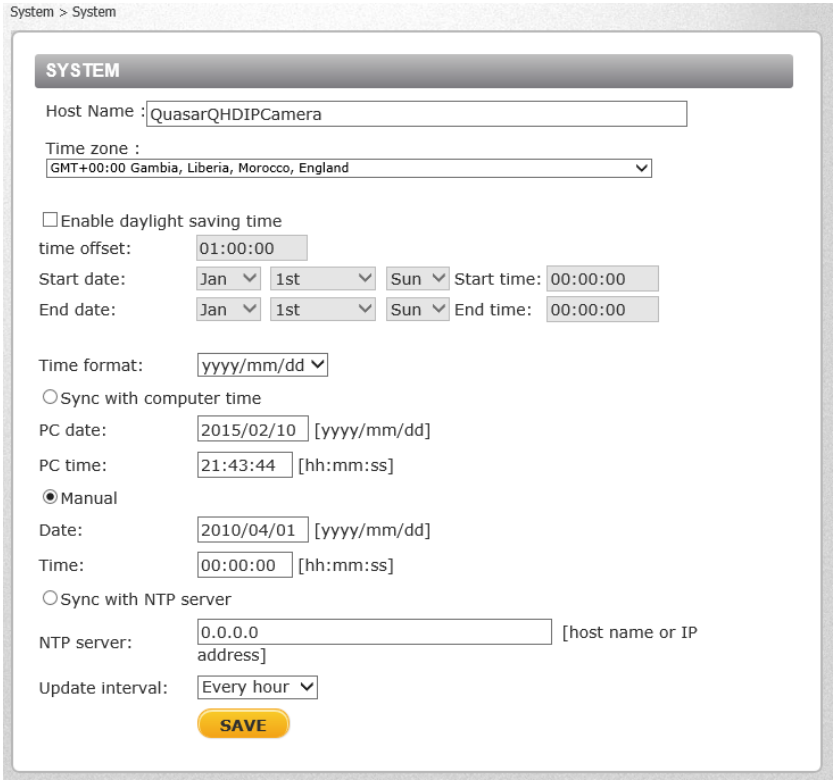


Figure 33: System Screen

The **System** screen includes the following fields:

Host Name

The host name is for camera identification. If the alarm function is enabled and is set to send an alarm message by Mail or FTP, the host name entered here is displayed in the alarm message. See Events Setup.

Time Zone

Select the time zone from the drop-down menu.

Enable Daylight Saving Time

To enable daylight saving time, check the box and then specify time offset (number of hours or minutes difference between daylight saving time and standard time), start date and time for daylight saving time, and end date and time for daylight saving time. The format for time offset is [hh:mm:ss]. For example, if the amount of time offset is one hour, enter 01:00:00 in the field.

Time format

Enables a choice of formats: either year, month and day (yyyy/mm/dd) or day, month and year (dd/mm/yyyy).

Sync with Computer Time

Select this button to synchronize video date and time display with the PC. You can change the PC date and time in the respective text box.

Manual

The Administrator can set video date and time manually. Entry format should be identical with that displayed to the right of the text box.

Sync with NTP Server

Network Time Protocol (NTP) is an alternate way to synchronize the camera's clock with an NTP server. Enter the network time server host name or IP address to synchronize in the text box. Then select an update interval (every hour, day or week) from the drop-down menu. For further information about NTP, visit www.ntp.org.

Click **Save** when finished.

9.3.2 Security

Clicking the **Security** tab in the **System** sidebar opens a drop-down menu with the following screens:

- User
- HTTPS
- IP Filter
- IEEE 802.1X

9.3.2.1 User

Click the **User** tab in the **Security** category on the sidebar to display user credentials.

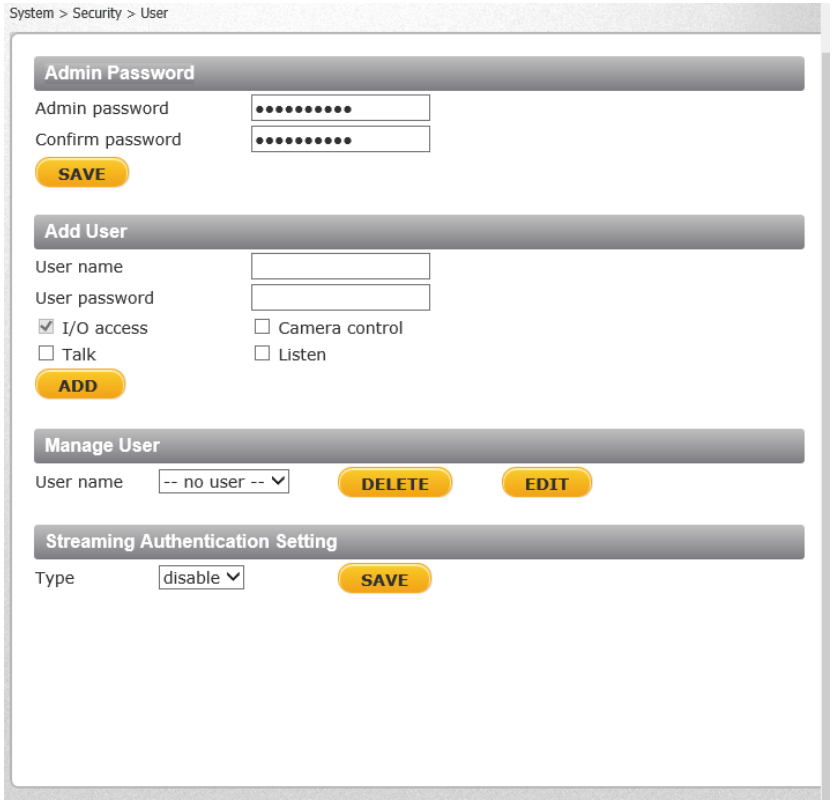


Figure 34: User Screen

Admin Password

Change the administrator's password by entering the new password in both text boxes. The input characters/numbers are displayed as dots for security purposes. After clicking **SAVE**, the web browser asks the Administrator for the new password (maximum 14 digits).

Note:
The following characters are valid: A-Z, a-z, 0-9,!#$%&'-.@^_~.

Add user

The user name and passwords are limited to 14 characters. There is a maximum of 20 user accounts.

To add a new user

1. Type the new user name and password in the respective fields.
2. Select the appropriate check boxes to give the user Camera Control, Talk and Listen permissions.
    - *I/O access* – Basic functions that enable you to view video when accessing to the camera.
    - *Camera control* – Allows you to change camera parameters on the **Camera** tab.
    - *Talk* – *Talk* allows the user at the local site to talk from the remote site to the administrator
    - *Listen* – *Listen* allows the user at the local site to listen from the remote site to the administrator.
3. Click **Add**.

Manage User

- To delete a user, click the *User name* drop-down list and select the user. Click **DELETE** to remove the user.
- To edit a user, click the *User name* drop-down list and select the user. Click **EDIT** to edit the user's password and privileges.

Note:
You must enter the user password and also select the authorized function(s).

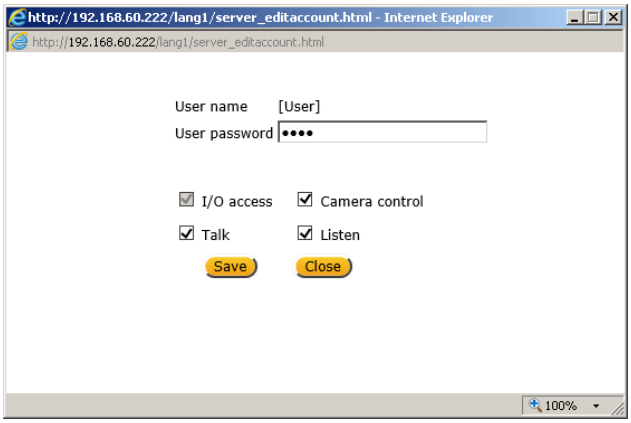


Figure 35: Edit User Account Dialog Box

- Click **Save** to modify the account credentials and privileges, or Close to discard changes.

Streaming Authentication Setting

From the drop-down list, select one of the following options:

- *Disable* – Do not use streaming authentication (default setting).
- *Basic* – A form of authentication that uses unencrypted base64 encoding. Basic Authentication should generally only be used where transport layer security, such as HTTPS, is provided.
- *Digest* – A form of authentication used over RTSP in which credentials are encrypted when transmitted.

Click **SAVE**.

9.3.2.2 HTTPS

To use HTTPS on the camera, an HTTPS certificate must be installed. The HTTPS certificate can be obtained either by creating and sending a certificate request to a Certificate Authority (CA) or by creating a self-signed HTTPS certificate as described below.

Note:
The self-signed certificate does not provide the same level of security as a CA-issued certificate.

HTTPS allows secure connections between the camera and web browser using Secure Socket Layer (SSL) or Transport Layer Security (TLS) to protect camera settings and username/password info. A self-signed certificate or a CA-signed certificate is required to implement HTTPS.

To create a self-signed certificate

Before a CA-issued certificate is obtained, users can first create and install a self-signed certificate. Under the **Security** category, click the **HTTPS** tab in the sidebar to display the following screen.

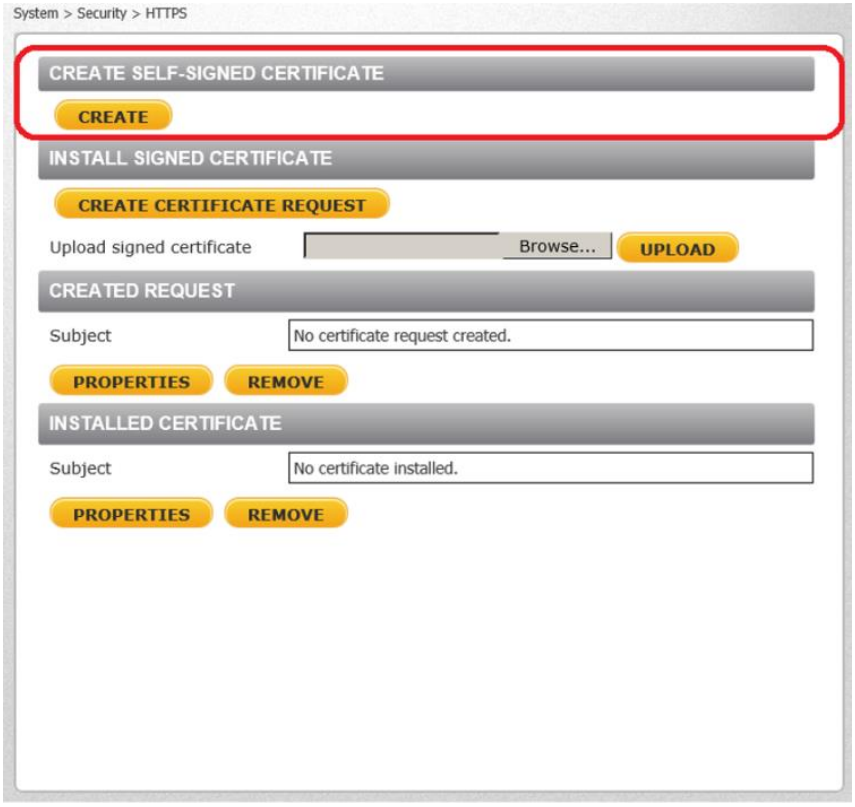


Figure 36: HTTPS Screen – Create Self-Signed Certificate

1. On the **HTTPS** page, click **CREATE** under *Create Self-Signed Certificate.* The **Create Self-Signed Certificate** dialog box opens.

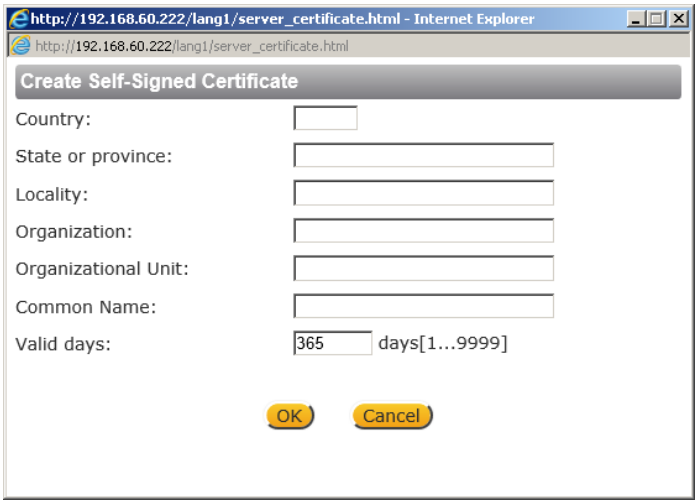


Figure 37: Create Self-Signed Certificate Dialog Box

2. Enter the information in the appropriate field. A definition of each of the required fields follows.
   - *Country* – Enter a two-letter combination code to indicate the specific country in which the certificate will be used. For instance, type "US" to indicate United States.
   - *State or province* – Enter the local administrative region.
   - *Locality* – Enter other geographical information.
   - *Organization* – Enter the name of the organization to which the entity identified in *Common Name* belongs.
   - *Organizational Unit* – Enter the name of the organizational unit to which the entity identified in the *Common Name* field belongs.
   - *Common Name* – Indicate the name of the person or other entity that the certificate identifies (often used to identify the website).
   - *Valid days* – Enter the period in days (1 ~ 9999) to indicate the valid period of certificate.
3. Click **OK** to save the certificate request after completion. The details are displayed in the *Subject* field of the *Installed Certificate* section.

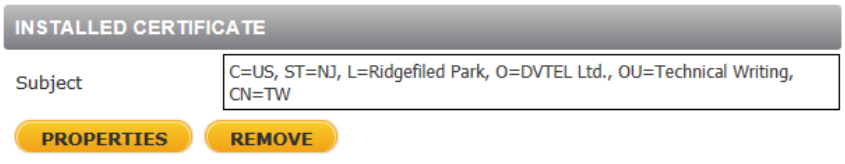


Figure 38: Installed Certificate Section

4. To view the details of the Installed Certificate, click **PROPERTIES**. The details are displayed in the **Certificate Properties** dialog box. If you want to remove the certificate, click **REMOVE**.

Certificate Properties

Certificate	
Version	2
Serial Number	0
Signature Algorithm	md5WithRSAEncryption
Issuer	C=US, ST=NJ, L=Ridgefiled Park, O=DVTEL Ltd., OU=Technical Writing, CN=TW
Validity	
Not Valid Before	Apr 6 13:22:49 2010 GMT
Not Valid After	Apr 6 13:22:49 2011 GMT
Subject	C=US, ST=NJ, L=Ridgefiled Park, O=DVTEL Ltd., OU=Technical Writing, CN=TW
Subject Public Key Info	
Public Key Algorithm	rsaEncryption
RSA Public Key	
Modulus (1024 bit)	ab 9c 89 37 ae bb a6 7b 35 7e f1 34 73 8c 00 59 a6 29 9e e4 61 d6 bd d5 e2 83 3e b9 4b df 5f ff d4 9b ca 52 fb 3c c2 fe 75 b5 f6 80 17 f3 f3 fc 8b 5d 55 c1 5b 9b 8b e7 1a 13 5d a8 1a a1 40 6f 83 2d 9c df 02 e7 c0 e1 89 7f 7c e0 7e 5f 7b e0 1c f9 fa bd a3 9c 37 4d 5a 98 c7 7e 3b 84 46 b9 c8 d5 d0 8e 79 c7 41 03 85 b2 2a c4 02 ef a2 f5 19 8b 01 e8 97 3a 3a df e2 48 5a 64 61 c4 7d 61
Exponent	65537
Signature	
Algorithm	md5WithRSAEncryption
Signature	54 f0 f6 bd c1 20 f4 98 24 1a 60 d7 66 ca a6 d4 f9 83 f0 90 36 df e4 e3 4e 21 5c 6b 0e 9a 43 fd 1e e6 bf f4 6a e4 ae 8a df e0 0d fb cb 48 8f 99 64 df c1 c2 9a a9 18 40 9f 4b c5 41 e5 ec 91 b1 04 8f 83 a2 cd f0 cd 49 4c e9 51 16 a9 1a af 3f 20 bf 77 4d e1 dd 5b 2a 43 e3 d4 35 c7 1e 5c 74 3c 1b f3 42 5f ab 91 65 e2 67 ea 6d

Figure 39: Certificate Properties

5. When the signed certificate is returned from the CA, click **Browse** in the *Install Signed Certificate* section to locate the file.

6. Click **UPLOAD** to install the certificate, as seen in Figure 40.

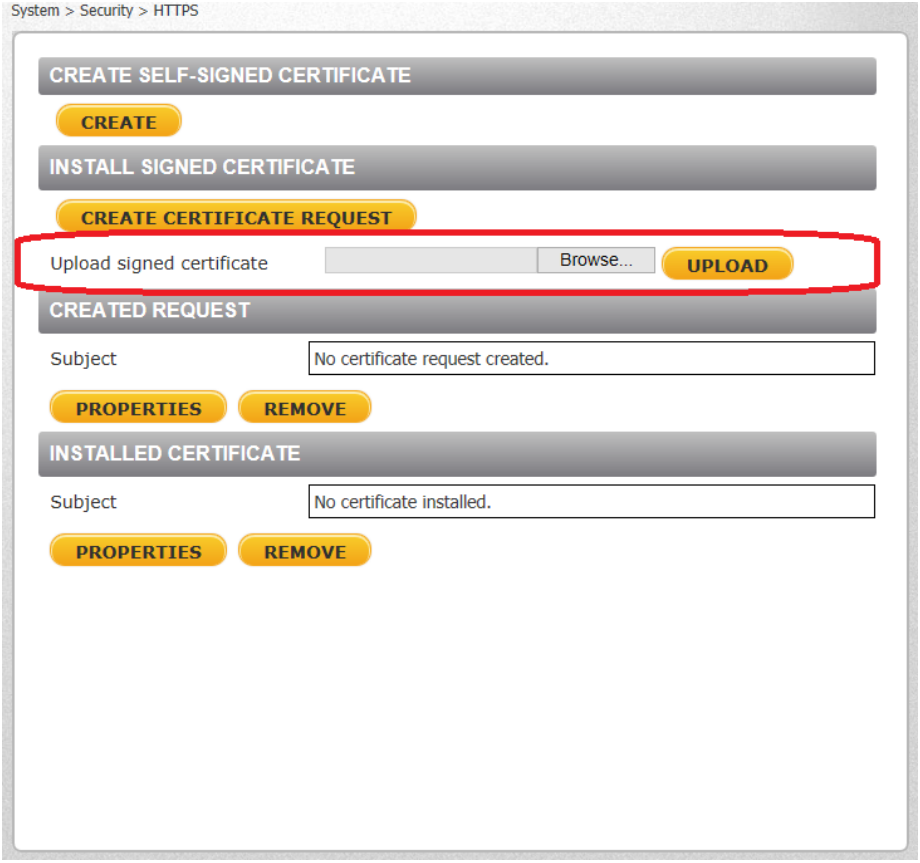


Figure 40: HTTPS Screen – Upload Signed Certificate

To create a certificate request

1. Click **CREATE CERTIFICATE REQUEST** to create and submit a certificate request in order to obtain a signed certificate from a CA.

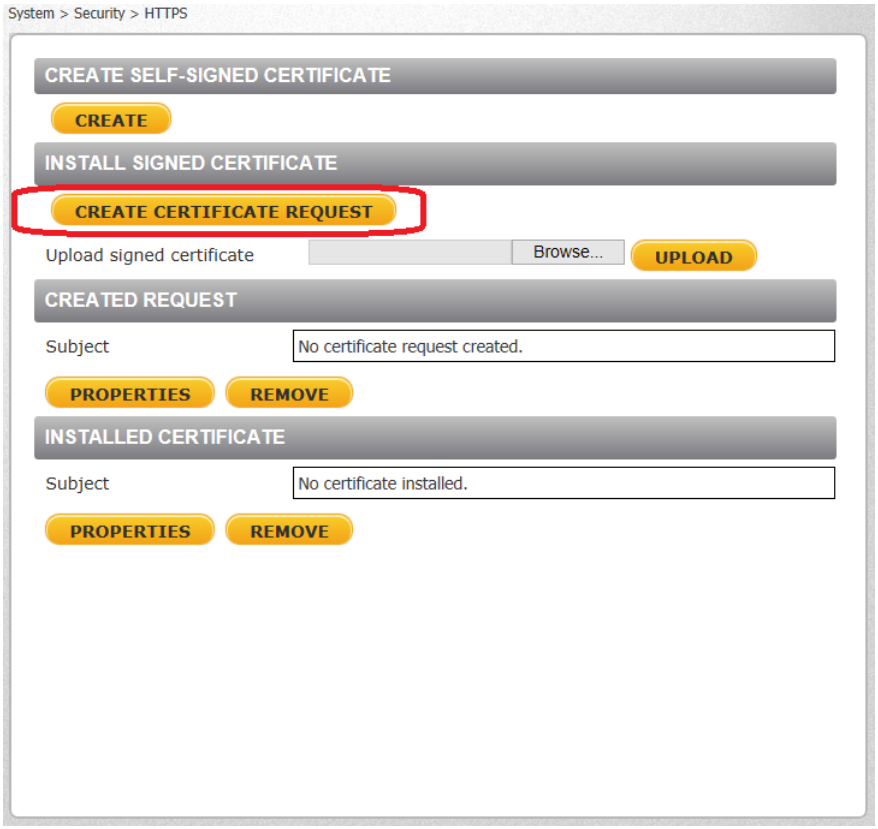


Figure 41: HTTPS Screen – Install Signed Certificate

The **Create Certificate Request** dialog box opens.

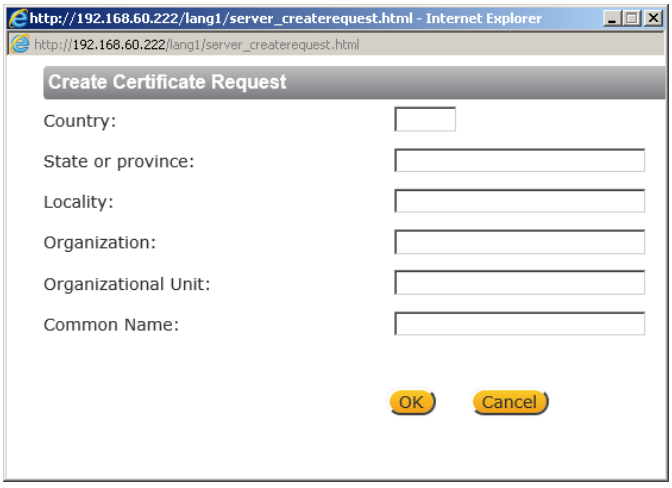


Figure 42: Create Certificate Request Dialog Box

2. Enter the information in the appropriate field. A definition of each of the required fields follows.
   - *Country* – Enter a two-letter combination code to indicate the specific country in which the certificate will be used. For instance, type "US" to indicate United States.
   - *State or province* – Enter the local administrative region.
   - *Locality* – Enter other geographical information.
   - *Organization* – Enter the name of the organization to which the entity identified in Common Name belongs.
   - *Organizational Unit* – Enter the name of the organizational unit to which the entity identified in the Common Name field belongs.
   - *Common Name* – Indicate the name of the person or other entity that the certificate identifies (often used to identify the website).
3. Click **OK** to save the details of the certificate request after completion. When the request is complete, the subject of the Created Request is displayed in the *Subject* field

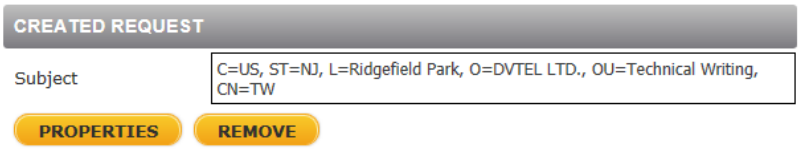


Figure 43: Created Request Subject

4. To view details of the Certificate Request, click **PROPERTIES** below the *Subject* field. The **Certificate Request Properties** dialog box opens. If you want to remove the certificate, click **REMOVE**.

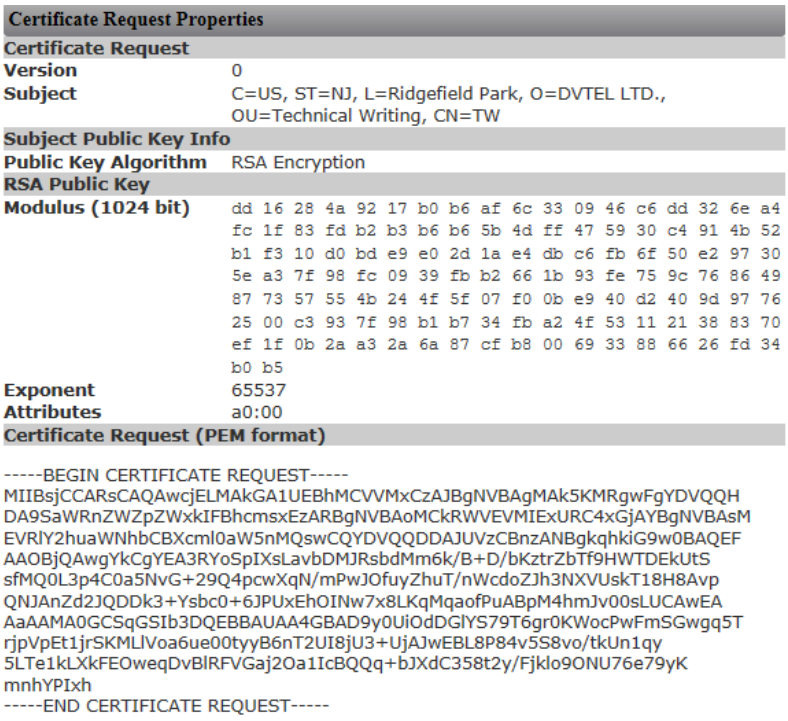

Certificate Request Properties
Certificate Request
Version 0
Subject C=US, ST=NJ, L=Ridgefield Park, O=DVTEL LTD., OU=Technical Writing, CN=TW
Subject Public Key Info
Public Key Algorithm RSA Encryption
RSA Public Key
Modulus (1024 bit) dd 16 28 4a 92 17 b0 b6 af 6c 33 09 46 c6 dd 32 6e a4 fc 1f 83 fd b2 b3 b6 b6 5b 4d ff 47 59 30 c4 91 4b 52 b1 f3 10 d0 bd e9 e0 2d 1a e4 db c6 fb 6f 50 e2 97 30 5e a3 7f 98 fc 09 39 fb b2 66 1b 93 fe 75 9c 76 86 49 87 73 57 55 4b 24 4f 5f 07 f0 0b e9 40 d2 40 9d 97 76 25 00 c3 93 7f 98 b1 b7 34 fb a2 4f 53 11 21 38 83 70 ef 1f 0b 2a a3 2a 6a 87 cf b8 00 69 33 88 66 26 fd 34 b0 b5
Exponent 65537
Attributes a0:00
Certificate Request (PEM format)
-----BEGIN CERTIFICATE REQUEST-----
MIIBsjCCARsCAQAwcjELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAk5KMRgwFgYDVQQH
DA9SaWRnZWZpZWxkIFBhcmsxEzARBgNVBAoMCkRWVEVMIExURC4xGjAYBgNVBAsM
EVRlY2huaWNhbCBXcml0aW5nMQswCQYDVQQDDAJUVzCBnzANBgkqhkiG9w0BAQEF
AAOBjQAwgYkCgYEA3RYoSpIXsLavbDMJRsbdMm6k/B+D/bKztrZbTf9HWTDEkUtS
sfMQ0L3p4C0a5NvG+29Q4pcwXqN/mPwJOfuyZhuT/nWcdoZJh3NXVUskT18H8Avp
QNJAnZd2JQDDk3+Ysbc0+6JPUxEhOINw7x8LKqMqaofPuABpM4hmJv00sLUCAwEA
AaAAMA0GCSqGSIb3DQEBBAUAA4GBAD9y0UiOdDGlYS79T6gr0KWocPwFmSGwgq5T
rjpVpEt1jrSKMLlVoa6ue00tyyB6nT2UI8jU3+UjAJwEBL8P84v5S8vo/tkUn1qy
5LTe1kLXkFEOweqDvBlRFVGaj2Oa1IcBQQq+bJXdC358t2y/Fjklo9ONU76e79yK
mnhYPIxh
-----END CERTIFICATE REQUEST-----

Figure 44: Certificate Request Properties Dialog Box

5. Copy the PEM-formatted request and send it to your CA.

> **Note:**
> The self-signed certificate does not provide the same high level of security as a certificate issued by a Certificate Authority (CA).

9.3.2.3 IP Filter

The IP filter restricts access to the camera by denying/allowing specific IP addresses. Click the **IP filter** tab under the category **Security** in the sidebar to display the following page.

Figure 45: IP Filter Screen

To enable the IP filter

1. Check the box to enable the IP filter function. Once enabled, the listed IP addresses (IPv4) are allowed or denied access to the camera.
2. Select *Allow* or *Deny* from the drop-down list.
3. Click **APPLY** to determine the IP filter behavior.

To add or delete an IP address

1. Enter the IP address in the *Filtered IP Addresses* text box.
2. Click **ADD** to add a new filtered address. The *Filtered IP Addresses* box shows the currently configured IP addresses. Up to 256 IP address entries may be specified.
3. To remove an IP address from the list, select the IP address and then click **DELETE**.

9.3.2.4 IEEE 802.1X

The camera is allowed to access a network protected by 802.1X/EAPOL (Extensible Authentication Protocol over LAN). Users must contact the network administrator to obtain certificates, user IDs, and passwords.

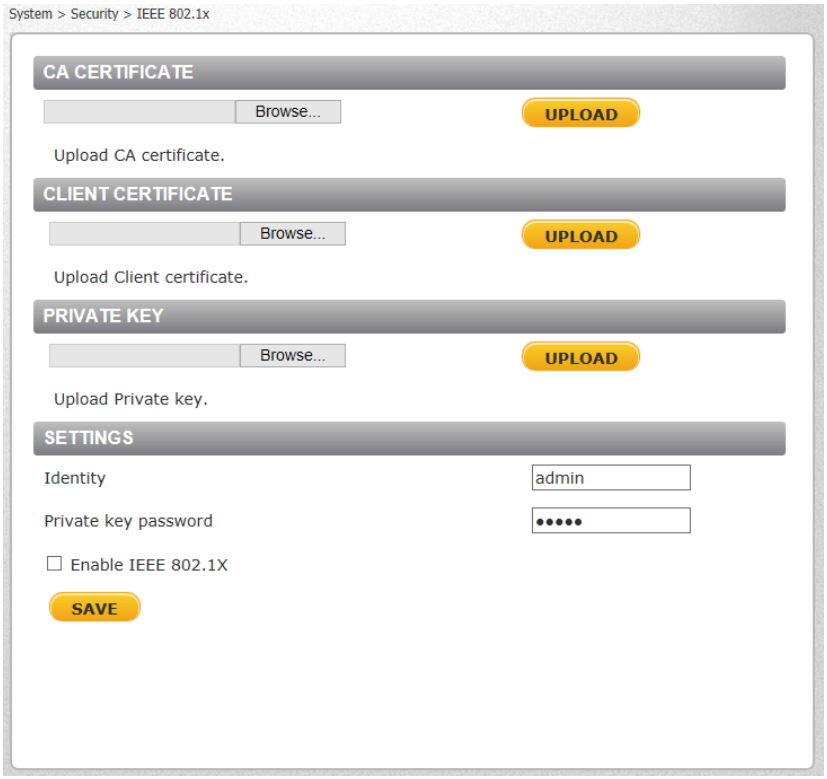


Figure 46: IEEE 802.1X/EAP-TLS Screen

CA Certificate

The CA certificate is created by the Certificate Authority for the purpose of validating itself. Click **Browse** to locate the file and **UPLOAD** to upload the certificate to check the server's identity.

Client Certificate

Upload the Client Certificate to authenticate the camera. Click **Browse** to locate the file and **UPLOAD** to upload the certificate.

Private Key

Upload the Private Key to authenticate the camera. Click **Browse** to locate the file and **UPLOAD** to upload the private key.

Settings

- *Identity* – Enter the user identity (user name) associated with the certificate. Up to 16 characters can be used.
- *Private Key Password* – Enter the password associated with the user identity. Up to 16 characters can be used.

Enable IEEE 802.1X

Select the checkbox to enable IEEE 802.1X security. Click **SAVE** to save the IEEE 802.1X/EAPTLS setting.

9.3.3 Network

From the **System** screen, click the **Network** tab.

The following screens are available from the **Network** tab:

- Basic • QoS • SNMP • UPnP • DDNS • Mail • FTP • HTTP

9.3.3.1 Basic

The **Basic** screen is used to configure the camera's basic network settings.

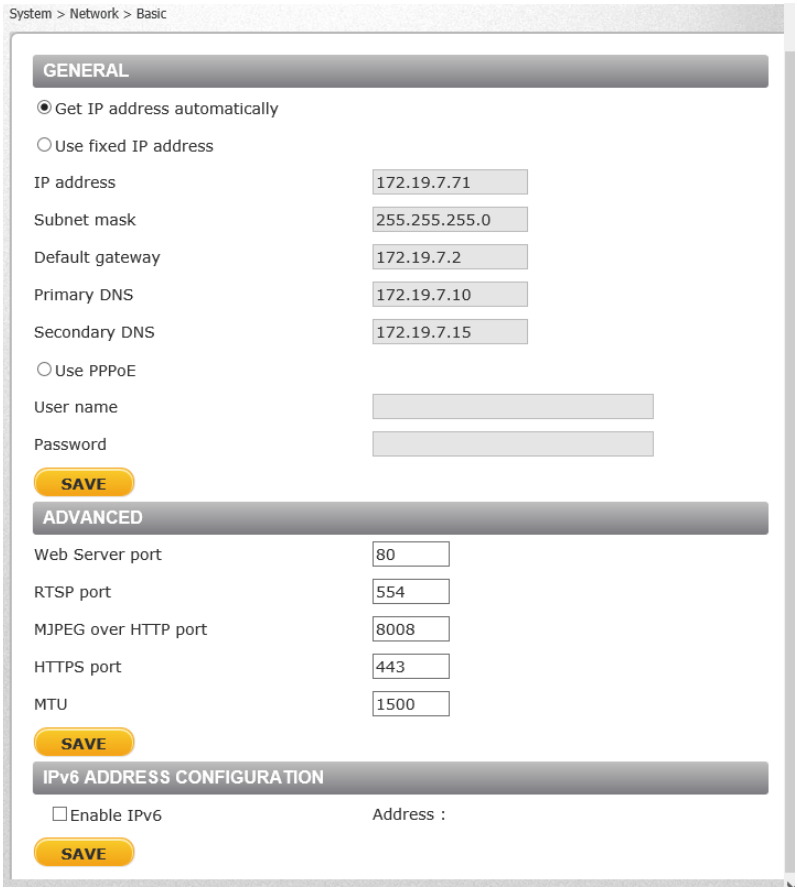


Figure 47: Network > Basic Screen

It is possible to connect to the camera with either fixed or dynamic (DHCP) IP address. The camera also provides PPPoE (Point-to-Point Protocol over Ethernet) support for users who connect to the network via PPPoE.

The **Basic** screen is divided into three sections: *General, Advanced* and *IPv6 Configuration*.

1. **General**

Select one of the following options in the *General* area for configuring network settings:

- Get IP address automatically
- Use fixed IP address
- User PPoE

- Get IP address automatically

If you select *Get IP address automatically*, you can use the DNA utility, which is provided in the supplied CD, to obtain the IP address from a DHCP server on the network. See Using the DNA Utility to Search and Access the Camera.

> **Note:**
> For future reference, record the camera's MAC address, which is found on the camera label.

- **Use fixed IP address**

The camera's default setting is *Use fixed IP address*. Refer to Using the DNA Utility to Search and Access the Camera for login with the default IP address. You may use DNA or enter the IP address in your Internet browser's URL address bar.

To set up a new static IP address

1. Select the *Use fixed IP address* option.
2. Enter the following information:
   - *IP address* – The IP address is necessary for network identification.
   - *Subnet mask* – Used to determine if the destination is in the same subnet. The default value is 255.255.255.0.
   - *Default gateway* – Used to forward frames to destinations in a different subnet. An invalid gateway setting causes transmission to destinations in other subnets to fail.
   - *Primary DNS* – The primary domain name server that translates host names into IP addresses.
   - *Secondary DNS* – A secondary domain name server that backs up the primary DNS.

- **Use PPPoE**

To use PPPoE

1. Enter your PPPoE user name and password into the respective fields.
2. Click **SAVE** to confirm the settings.

2. **Advanced**

Enter the following advanced parameters in the *Advanced* section of the screen:

- *Web Server port* – The default web server port is 80. Once the port is changed, the user must be notified the change for the connection to be successful. For instance, when the Administrator changes the HTTP port of the camera whose IP address is 192.168.0.100 from 80 to 8080, the user must type in the web browser http://192.168.0.100:8080 instead of http://192.168.0.100.
- *RTSP port* – The default setting of the RTSP port is 554. The range is from 1024 to 65535.
- *MJPEG over HTTP port* – The default setting of MJPEG over HTTP port is 8008. The range is from 1024 to 65535.
- *HTTPS port* – The default setting of HTTPS port is 443. The range is from 1024 to 65535.
- *MTU* – The MTU (Maximum Transmission Unit) is the greatest amount of data that can be transferred in one physical frame on the network. For Ethernet, the MTU is *1500* bytes (default setting). For PPPoE, the MTU is *1492*. The range is from *700* to *1500* bytes.

Note:
Be sure to assign a different port number for each service mentioned above.

Click **SAVE** to save the settings.

3. **IPv6 Address Configuration**

IPv6 is not supported.

9.3.3.2 QoS

QoS (Quality of Service) provides differentiated service levels for different types of traffic packets and guarantees delivery of priority services during periods of network congestion. Adapting the Differentiated Services (DiffServ) model, traffic flows are classified and marked with DSCP (DiffServ Code point) values, and as a result receive the corresponding forwarding treatment from DiffServ-capable routers. DSCP configuration settings are entered in the **System > Network > QOS** screen:

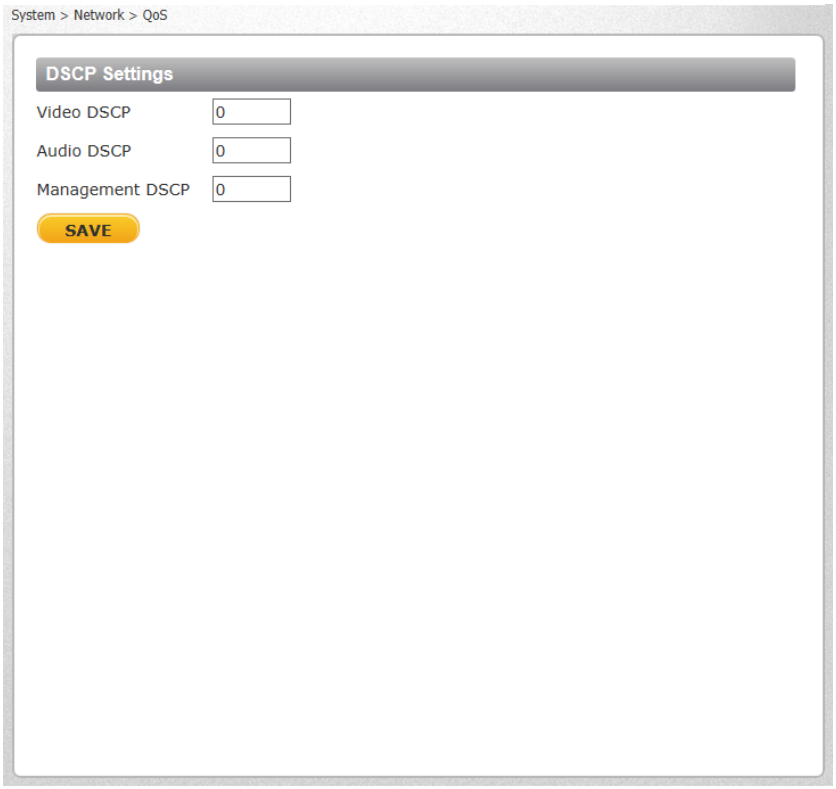


Figure 48: QoS Screen

DSCP Settings

The DSCP value range is from 0 to 63. The default DSCP value is 0 (DSCP disabled). The camera uses the following QoS classes: Video, Audio, and Management.

- *Video DSCP* – This class consists of applications such as MJPEG over HTTP, RTP/RTSP and RTSP/HTTP.
- *Audio DSCP* – The camera supports audio.
- *Management DSCP* – This class consists of HTTP traffic (web browsing).

Click **SAVE** when complete.

Note:
To enable this function, make sure the switches/routers in the network support QoS.

9.3.3.3 SNMP Settings

The Simple Network Management Protocol (SNMP) enables the camera to be monitored and managed remotely by the network management system. SNMP configuration settings are entered in the **System > Network > SNMP** screen.

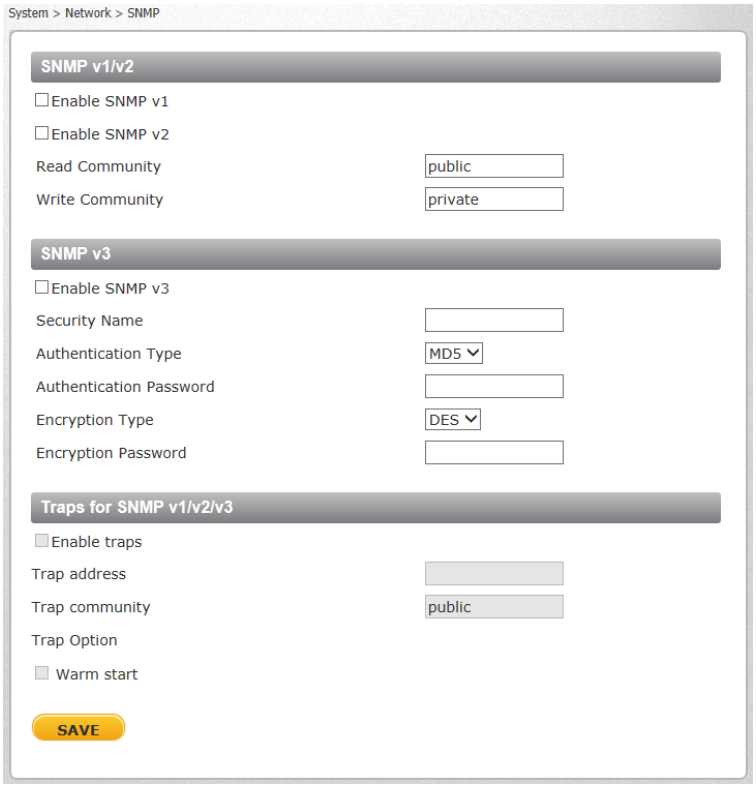


Figure 49: SNMP Settings Screen

SNMP v1/v2

- *Enable SNMP v1* or *Enable SNMP v2* – Select the version of SNMP (v1 or v2) to use by checking the relevant box.
- *Read Community* – Specify the community name that has read-only access to all supported SNMP objects. The default value is *public.*
- *Write Community* – Specify the community name that has read/write access to all supported SNMP objects (except read-only objects). The default value is *private.*

SNMP v3

SNMP v3 provides important security features including:

- Confidentiality – Encryption of packets to prevent snooping by an unauthorized source.
- Integrity – Message integrity to ensure that a packet has not been tampered with in transit including an optional packet replay protection mechanism.
- Authentication – To verify that the message is from a valid source.

To enable the SNMP v3 protocol, enter the appropriate data and passwords requested:

- *Enable SNMP v3* – Select the checkbox.
- *Security Name* – See note below.
- *Authentication Type* – Select MD5 or SHA from the drop-down list. See note below.
- *Authentication Password* – See note below.
- *Encryption Type* – Select DES or AES from the drop-down list. See note below.
- *Encryption Password* – See note below.

Note:
You may have to consult with your System Administrator to activate this function.

Traps for SNMP v1/v2/v3

Traps are used by the camera to send messages to a management system for important events or status changes.

- *Enable traps* – Check this box to activate trap reporting.
  - *Trap address* – Enter the IP address of the management server.
  - *Trap community* – Enter the community to use when sending a trap message to the management system. The default value is *public*.
- Trap Option
  - *Warm start* – A warm start SNMP trap signifies that the SNMP device, such as the camera, performs a software reload.

Click **SAVE** when complete.

9.3.3.4 UPnP

The **System > Network > UPnP** screen enables the Universal Plug-and-Play protocol on your network devices.

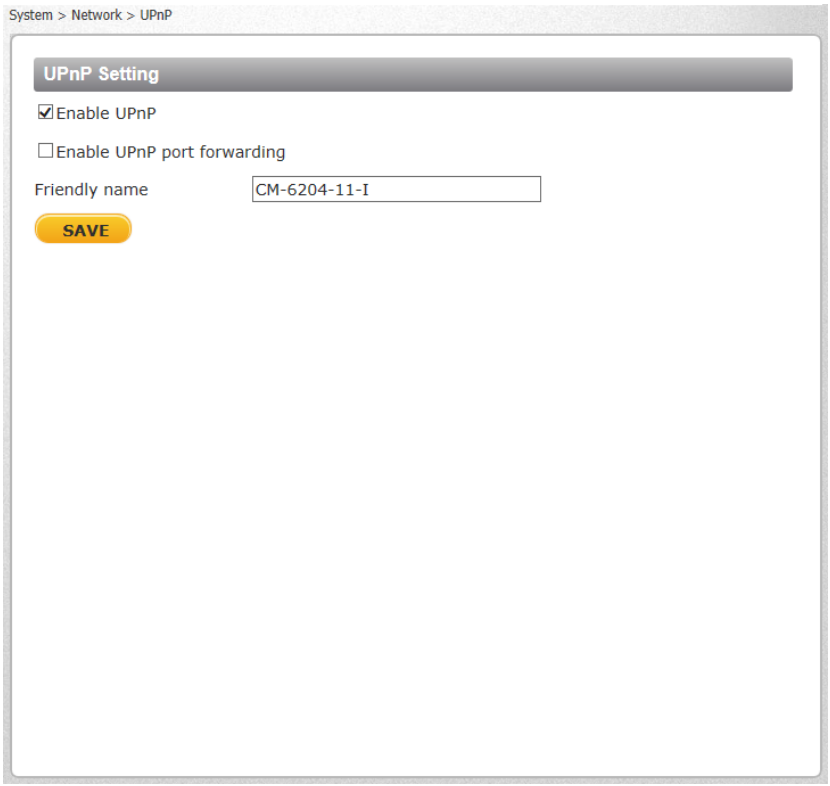


Figure 50: UPnP Screen

UPnP Settings

- *Enable UPnP* – If UPnP is enabled and a camera is discovered on the LAN, the icon of the connected camera appears in **My Network Places**, allowing direct access, as seen below.

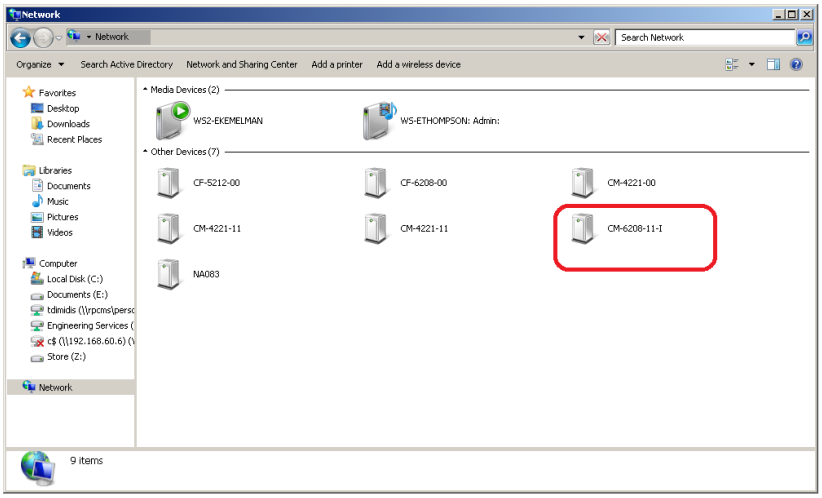


Figure 51: Direct Access to Camera with UPnP Enabled

Note:
To enable this function, make sure the UPnP component is installed on your computer. Refer to Install UPnP Components for the Windows 7, Windows 8, and Windows 8.1 procedure.

- *Enable UPnP port forwarding* – When UPnP port forwarding is enabled, the camera is allowed to open the web server port on the router automatically.

> **Note:**
> To enable this function, make sure that your router supports UPnP and that it is activated.

- *Friendly name* – Enter the name for the camera for identification.

Click **SAVE** to save the settings.

9.3.3.5 DDNS

Dynamic Domain Name System (DDNS) allows a host name to be constantly synchronized with a dynamic IP address. This permits those using a dynamic IP address to be accessed by a static domain name. DDNS configuration settings are entered in the **System > Network > DDNS** screen:

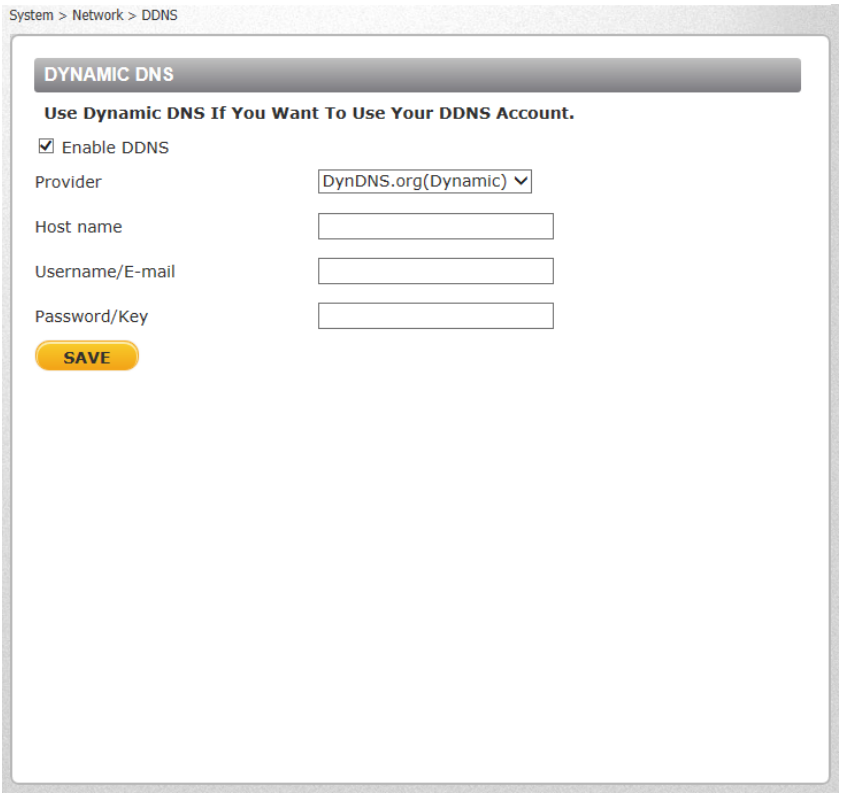


Figure 52: DDNS Screen

To use DDNS

1. Select the *Enable DDNS* checkbox.
2. From the *Provider* drop-down list, select a DDNS host provider name.
3. In the *Host name* text box, enter the registered domain name.
4. In the *Username/E-mail* text box, enter the username or e-mail address required by the DDNS provider for authentication.
5. In the *Password/Key* text box, enter the password or key required by the DDNS provider for authentication.

Click **SAVE** to save the setting.

9.3.3.6 Mail

Simple Mail Transfer Protocol (SMTP) is a protocol for sending e-mail messages between servers. It is a relatively simple, text-based protocol, where a text message is transferred to one or more specified recipients. The Administrator can send an e-mail via Simple Mail Transfer Protocol (SMTP) when an alarm is triggered. E-mail notifications are set by selecting the checkbox for an e-mail-related triggered action on the IO, Network Failure Detection, Tampering, Periodic Event, Manual trigger, and Motion Detection screens.

SMTP (E-mail) server configuration settings are entered in the **System > Network > Mail** screen:

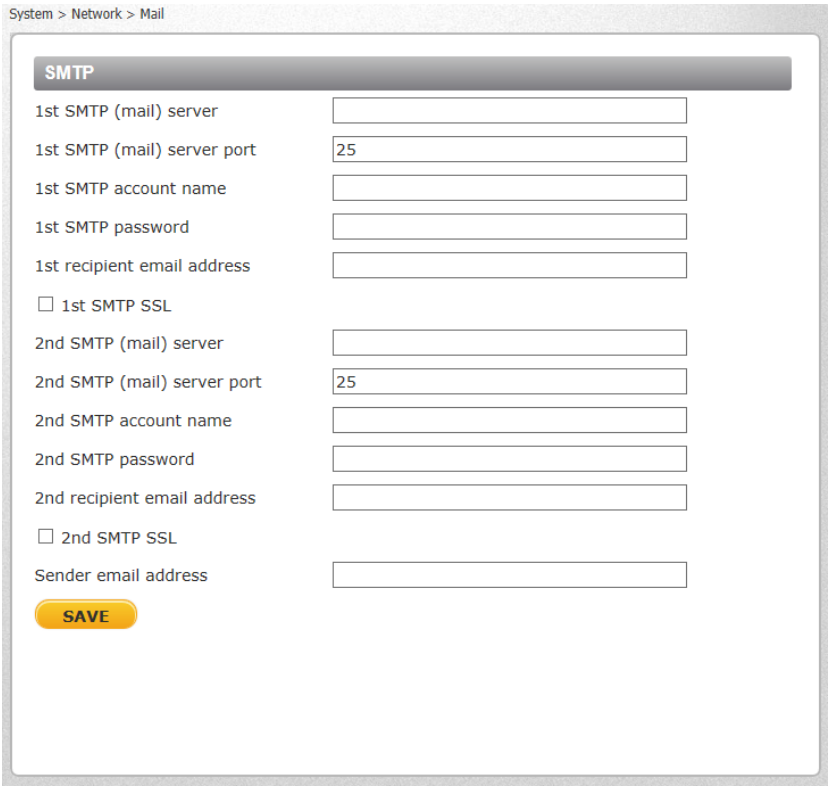


Figure 53: Mail Screen – SMTP

Two SMTP server accounts can be configured with or without SSL encryption. Enter the settings for the 1st SMTP server and 2nd SMTP server in the appropriate fields. Settings include SMTP server, server port (the default port is 25), account name, password, and recipient e-mail address settings. To encrypt e-mail with SSL, select the *1st SMTP SSL* and/or *2nd SMTP SSL* checkbox. For SMTP server details, contact your network service provider. Click **SAVE** when finished.

9.3.3.7 FTP

The Administrator can send an alarm message to one or two File Transfer Protocol (FTP) sites when motion is detected. FTP notifications are set by selecting the checkbox for an FTP-related triggered action on the IO, Network Failure Detection, Tampering, Periodic Event, Manual trigger, and Motion Detection screens.

For each server, enter the server IP address, server port number, user name, password, and remote folder path. Settings are entered in the **System > Network > FTP** screen:

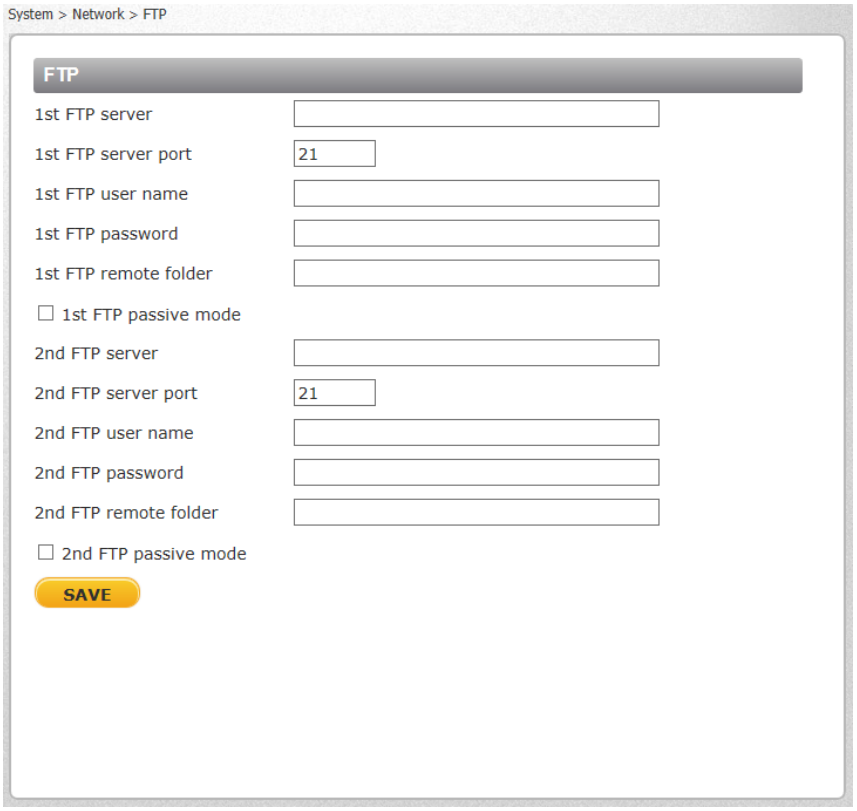


Figure 54: FTP Screen

To use passive mode, select the *1st FTP passive mode* or *2nd FTP passive mode* checkbox for the respective server. In passive mode, FTP the client initiates both connections to the server, solving the problem of firewalls filtering the incoming data port connection to the client from the server.

In order to support passive mode FTP on the server-side firewall, the following communication channels must be opened:

- FTP server's port 21 from anywhere (client initiates connection)
- FTP server's port 21 to ports > 1023 (server responds to client's control port)
- FTP server's ports > 1023 from anywhere (client initiates data connection to random port specified by server)
- FTP server's ports > 1023 to remote ports > 1023 (server sends ACKs and data to client's data port)

Click **SAVE** when finished.

9.3.3.8 HTTP

An HTTP notification server detects notification messages of triggered events sent from cameras. HTTP notifications are set by selecting the *Send HTTP notification* checkbox on the IO, Tampering, Manual trigger, and Motion Detection screens.

Two notification server accounts (Alarm Triggered and Motion Detection) can be set up and sent to the specified HTTP servers. For each server, enter the HTTP details, including server IP address, user name, and password. Settings are entered in the **System > Network > HTTP** screen:

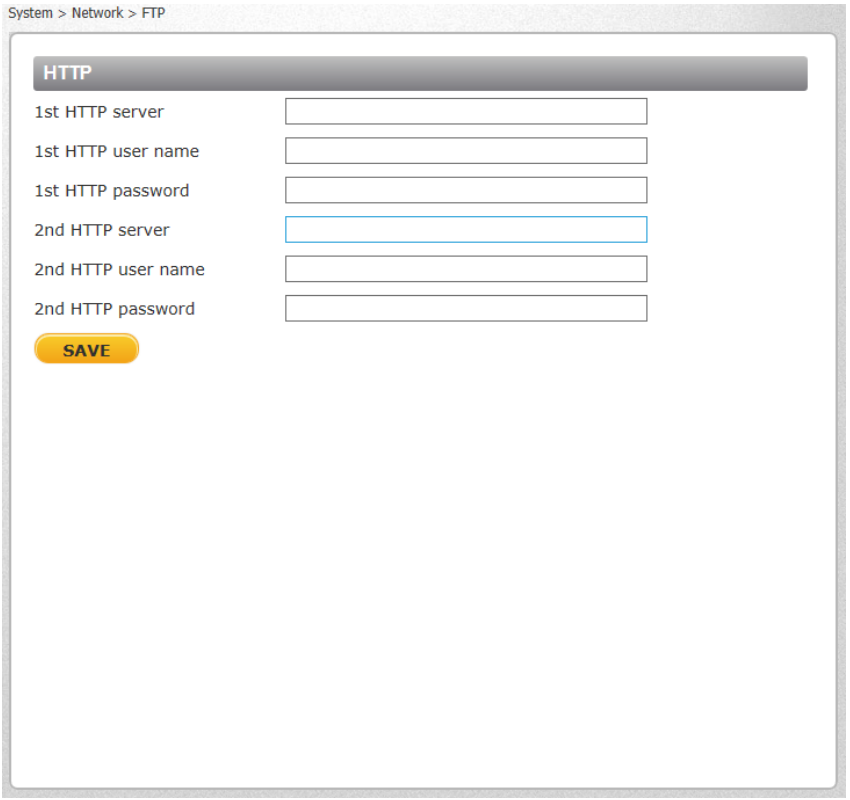


Figure 55: HTTP Screen

Click **SAVE** when finished.

9.3.4 Events Setup

The **Events Setup** tab includes the following screens:

- IO
- Network Failure Detection
- Tampering
- Day/Night Trigger
- Periodic Event
- Manual Trigger

9.3.4.1 IO

The **IO** screen is used to control input and output alarms and messages, which are generated when an event is recognized by the system.

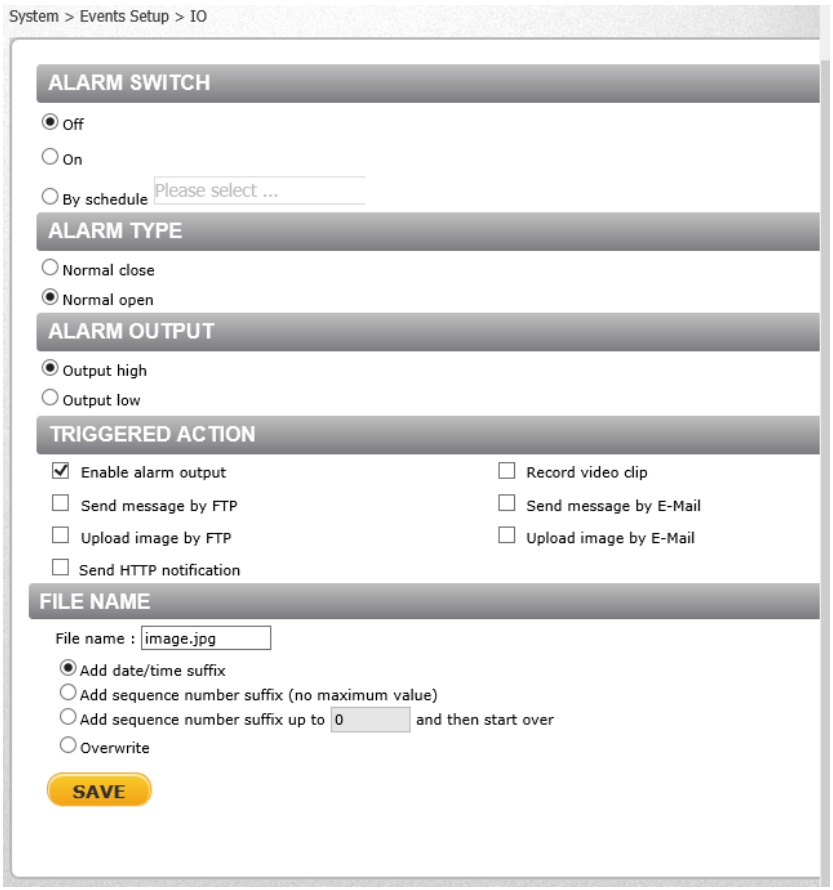


Figure 56: IO Screen

9.3.4.1.1 *Alarm Switch*

The Administrator can select from the following options:

- Select *Off* to disable an alarm.
- Select *On* to enable an alarm (default setting).
- Select *By Schedule* to set a schedule. Then click *Please Select* to select up to 10 schedules from the drop-down list that opens. The selected schedules are displayed in the *Please Select* text box. To set a schedule, open the Schedule tab.

Click **Save** after configuring the settings.

9.3.4.1.2 *Alarm Type*

Select an alarm type (*Normal close* or *Normal open*) that corresponds to the alarm application. *Normal open* is the default setting. Click **SAVE** after configuring the settings.

9.3.4.1.3 *Alarm Output*

Define the normal alarm output signal as *Output high* or *Output low*, according to the current alarm application. *Output high* is the default setting. Click **SAVE** after configuring the settings.

9.3.4.1.4 *Trigger Action*

The Administrator can specify various alarm actions to take when an alarm is triggered. The following options are available:

- *Enable alarm output* – Select this checkbox to enable alarm relay output (default setting).
- *Send message by FTP* – Select the checkbox send an alarm message by FTP when an alarm is triggered.
- *Upload image by FTP* – Select this box to assign an FTP site and configure the parameters shown. When an alarm is triggered, event images are uploaded to the designated FTP site.

> **Note:**
> Images can be sent by FTP only when MJPEG is selected as the video stream from the Video Format screen.

Follow these steps:

- From the *FTP address* drop-down list, select one of the two FTP addresses to use.
- From the *Pre-trigger buffer* and *Post-trigger buffer* drop-down lists, select the number of frames for the buffer from 1-20 frames.

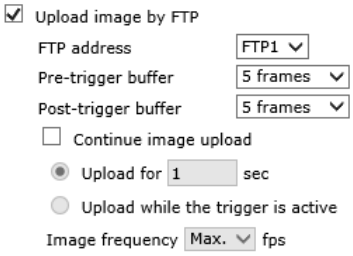


Figure 57: Upload Image by FTP

- Select the *Continue image upload* checkbox to upload an image by FTP for a defined period of time or while the trigger is active. Select one of the following options:
  - To specify the length of time for the upload, select *Upload for* and enter the number of seconds in the text box.
  - To upload while the trigger is active, select *Upload while the trigger is active*.

  In the *Image Frequency* text box, from the drop-down list select the number of frames per seconds from 1-15 for the upload.

> **Note:**
> Make sure that FTP configuration has been completed. See FTP for details.

- *Send HTTP notification* – Select this checkbox to send a notification by HTTP. Select the destination HTTP address from the drop-down menu and specify the parameters for event notifications by the IO event triggered. When an alarm is triggered, the notification will be sent to one of two specified HTTP servers. See figure below.

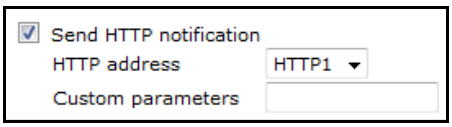


Figure 58: Send HTTP Notification

- *Record video clip* – Select this box in order to save the alarm-triggered recording to your microSDXC card or to the NAS. Enter the number of seconds for the pre-trigger buffer. Select the first radial button if you wish to upload for a specified length of time and enter the number of seconds. Alternatively, select the second radial button to upload during the active trigger.

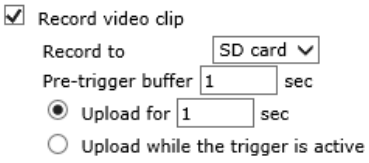


Figure 59: Record Video Clip

Note:
In order to use this function, make sure that local recording with a microSDXC card is activated and that the NAS is properly configured. See Recording for further details.

- *Send message by E-Mail* – Select the checkbox send an alarm message by e-mail when an alarm is triggered. The e-mail address is entered in the Mail screen.
- *Upload image by E-Mail* – Select this checkbox to assign an e-mail address for sending the image captured by a triggered alarm. The e-mail address is entered in the Mail screen.

Note:
Images can be sent by e-mail only when MJPEG is selected as the video stream from the Video Format screen.

  - From the *E-Mail address* drop-down list, select one of the two e-mail addresses.
  - From the *Pre-trigger buffer* and *Post-trigger buffer* drop-down lists, select the number of frames for the buffer from 1-20 frames.

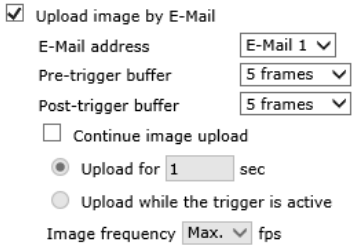


Figure 60: Upload Image by E-Mail

- Check the *Continue image upload* box if you wish to upload an image by e-mail for a defined period of time or while the trigger is active. Select one of the following options:
  - To specify the length of time for the upload, select *Upload for* and enter the number of seconds in the text box.
  - To upload while the trigger is active, select *Upload while the trigger is active*.

  In the *Image Frequency* text box, from the drop-down list select the number of frames per seconds from 1-15 for the upload.

  Note:
  Make sure that SMTP configuration has been completed. See Mail for details.

Click **SAVE** after configuring the settings.

9.3.4.1.5 *File Name*

- *File Name* – Enter a file name in the field, for example *image.jpg.* The uploaded image's file name format is set in this section. Select one that meets your requirements.
- Add date/time suffix (default setting)
  File name: imageYYMMDD_HHNNSS_XX.jpg
  Y: Year, M: Month, D: Day
  H: Hour, N: Minute, S: Second
  X: Sequence Number
- Add sequence number suffix (no maximum value)
  File name: imageXXXXXXX.jpg
  X: Sequence Number
- Add sequence number suffix (limited value)
  File Name: imageXX.jpg
  X: Sequence Number

  The file name suffix ends at the number being set. For example, if the setting is up to "10," the file name will start from 00, end at 10, and then start over again.
- Overwrite
  The original image in the FTP site will be overwritten by the new uploaded file with a static filename.

Click **SAVE** after configuring the settings.

9.3.4.2 Network Failure Detection

Settings on the **Network Failure Detection** screen enable the camera to periodically ping another IP device within the network to detect a network failure, for example, if a video server is disconnected. By implementing local recording through a microSDXC card, the camera can operate as a backup recording device for the surveillance system if network communication is lost due to a network failure.

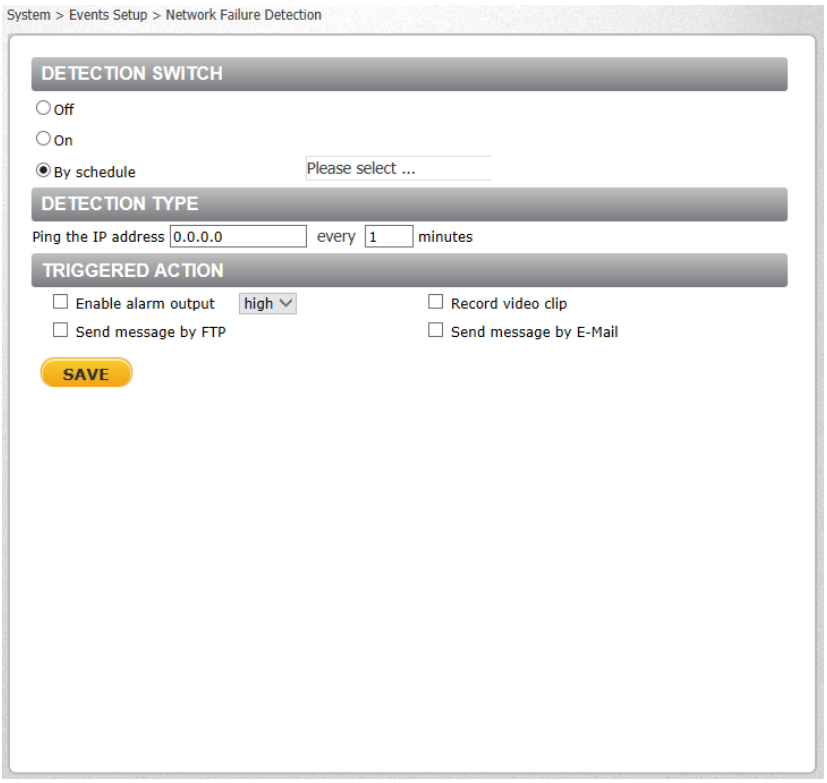


Figure 61: Network Failure Detection Screen

9.3.4.2.1 *Detection Switch*

The Administrator can select from the following options:

- Select *Off* to disable an alarm (default setting).
- Select *On* to enable an alarm.
- Select *By Schedule* to set a schedule. Then click *Please Select* to select up to 10 schedules from the drop-down list that opens. The selected schedules are displayed in the *Please Select* text box. To set a schedule, open the Schedule tab.

Click **SAVE** after configuring the settings.

9.3.4.2.2 *Detection Type*

In the text box, enter the IP address to ping and the time interval (in minutes) between pings. Click **SAVE** after configuring the settings.

9.3.4.2.3 *Triggered Action*

The Administrator can specify various alarm actions to be taken when an alarm is triggered. The options are listed below.

- *Enable alarm output* – Check this box and select the predefined type of alarm output *(low* or *high*) to enable alarm relay when a network failure is detected.
- *Send message by FTP* – Select whether to send an alarm message by FTP when a network failure is detected.
- *Record video clip* – Select this box in order to save the alarm-triggered recording into a microSDXC card or the NAS. Enter the number of seconds for the pre-trigger buffer. Select the first radial button to upload for a specified length of time and enter the number of seconds. Alternatively, select the second radial button to upload during the active trigger. See Figure 59: Record Video Clip.

> **Note:**
> In order for this function to be implemented, make sure that local recording with a microSDXC card is activated and that the NAS is properly configured. See Recording for further details.

- *Send message by E-Mail* – Select whether to send an alarm message by e-mail when a network failure is detected.

Click **SAVE** to save the network failure detection settings.

9.3.4.3 Tampering

The **Tampering** screen enables the camera to deal with tampering (such as deliberate redirection, blocking, paint-spraying, and obscuring the lens, etc.). Using video analysis, the camera can react to such events by sending notifications or uploading snapshots to the specified destination(s).

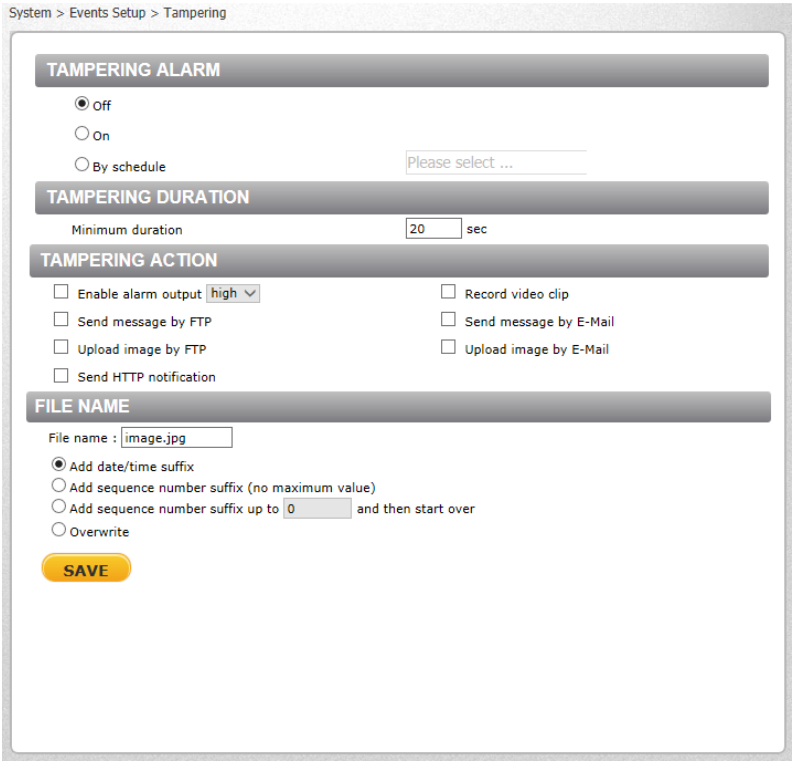


Figure 62: Tampering Screen

Detection of camera tampering is achieved by measuring the differences between the older frames of video (which are stored in buffers) and more recent frames.

9.3.4.3.1 *Tampering Alarm*

The Administrator can select from the following options:

- Select *Off* to disable the tampering alarm (default setting).
- Select *On* to enable the tampering alarm.
- Select *By Schedule* to set a schedule. Then click *Please Select* to select up to 10 schedules from the drop-down list that opens. The selected schedules are displayed in the *Please Select* text box. To set a schedule, open the Schedule tab.

Click **Save** after configuring the settings.

9.3.4.3.2 *Tampering Duration*

Minimum tampering duration is the time for video analysis to determine whether camera tampering has occurred. Minimum duration can also be interpreted as defining the tampering threshold; a longer duration represents a higher threshold.

In the *Minimum duration* text box, enter the tampering duration time in seconds. The range is from 10 to 3600 seconds.

9.3.4.3.3 *Tampering Action*

The Administrator can specify multiple alarm actions to be taken when tampering is detected. The options are listed as follows:

- *Enable alarm output* – Check this box and select the predefined type of alarm output *(high* or *low*) to enable alarm relay when tampering is detected.
- *Send Message by FTP* – The Administrator can select whether to send an alarm message by FTP when tampering is detected.
- *Upload Image by FTP* – Selecting this option enables you to assign an FTP site and configure various parameters, as seen in Figure 57: Upload Image by FTP. When tampering is detected, event images will be uploaded to the designated FTP site.

  Note:
  Images can be sent by FTP only when MJPEG is selected as the video stream from the Video Format screen.

  Specify the FTP address to use from the drop-down menu. Select the number of frames for the pre-trigger and post-trigger buffers from the drop-down menu of 1-20 frames.

  Check the box for *Continue image upload if* you wish to use this option. To specify the length of time for the upload, click this radial button and enter the number of seconds. To upload while the trigger is active, click this radial button.

  Finally, select the number of frames per second from the drop-down menu next to *Image frequency*.

- *Send HTTP notification* – Check this option, select the destination HTTP address, and specify the parameters for HTTP notifications. When the tampering alarm is triggered, the HTTP notifications can be sent to the specified HTTP server. See Figure 58: Send HTTP Notification.

- *Record video clip* – Select this box in order to save the alarm-triggered recording into a microSDXC card. Enter the number of seconds for the pre-trigger buffer. Select the first radial button to upload for a specified length of time and enter the number of seconds. Alternatively, select the second radial button to upload during the active trigger. See Figure 59: Record Video Clip.

> **Note:**
> In order for this function to be implemented, make sure that local recording with a microSDXC card is activated and that the NAS is properly configured. See Recording for further details.

- *Send message by E-Mail* – The Administrator can select whether to send an alarm message by e-mail when tampering is detected.
- *Upload Image by E-Mail* – Selecting this option enables you to assign an e-mail address and configure various parameters, as shown in Figure 60: Upload Image by E-Mail. When tampering is detected, event images will be sent to the designated e-mail address.

> **Note:**
> Images can be sent by e-mail only when MJPEG is selected as the video stream from the Video Format screen.

Select one of two e-mail addresses from the drop-down menu. Select the number of frames for the pre-trigger and post-trigger buffers from the drop-down menu of 1-20 frames.

Check the box for *Continue image upload* if you wish to use this option. To specify the length of time for the upload, click this radial button and enter the number of seconds. To upload while the trigger is active, click this radial button. Finally, select the number of frames per second from the drop-down menu next to *Image frequency.*

> **Note:**
> Make sure SMTP or FTP configuration has been completed. See the Mail and FTP sections for further details.

9.3.4.3.4 *File Name*

- *File Name* – Enter a file name in the field, for example *image.jpg.* The uploaded image's file name format is set in this section. Select one that meets your requirements.
- Add date/time suffix (default setting)
  File name: imageYYMMDD_HHNNSS_XX.jpg
  Y: Year, M: Month, D: Day
  H: Hour, N: Minute, S: Second
  X: Sequence Number
- Add sequence number suffix (no maximum value)
  File name: imageXXXXXXX.jpg
  X: Sequence Number
- Add sequence number suffix (limited value)
  File Name: imageXX.jpg
  X: Sequence Number

  The file name suffix ends at the number being set. For example, if the setting is up to "10," the file name will start from 00, end at 10, and then start over again.

- Overwrite
  The original image in the FTP site will be overwritten by the new uploaded file with a static filename.

Click **SAVE** after configuring the settings.

9.3.4.4 Day/Night Trigger

The **Day/Night Trigger** screen is used to enable the camera to trigger a device connected to the camera's alarm output when the camera switches to *Day* or *Night* mode, which is set on the IR Function screen.

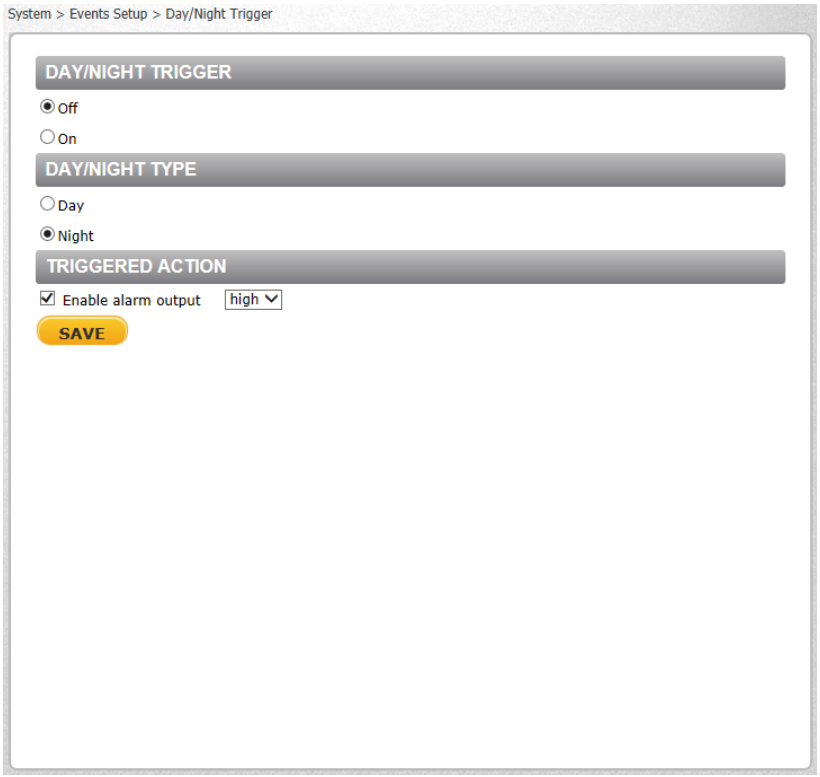


Figure 63: Day/Night Trigger Screen

In the *Day/Night Trigger* section, select *On* to enable the Day/Night Trigger or *Off* to disable it.

In the *Day/Night Type* section, select *Day* when the camera enters Day mode, for example to deactivate an external device, such as a lighting source. Select *Night* to activate an external device when the camera enters Night mode.

In the *Triggered Action* section, check *Enable alarm output* to activate an external lighting source. Depending on the voltage requirements of the external device, from the drop-down menu select *high* or *low*.

9.3.4.5 Periodic Event

The **Periodic Event** screen is used to specify an alarm to be triggered at a specified time interval.

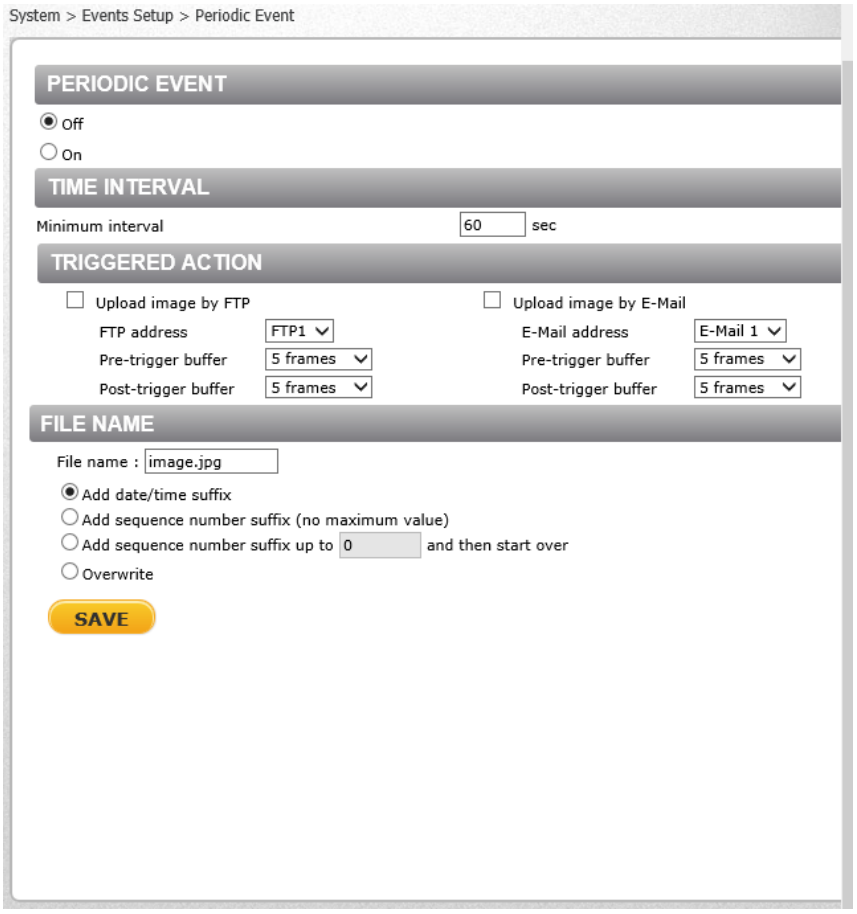


Figure 64: Periodic Event Screen

9.3.4.5.1 *Periodic Event*

Select *Off* or *On* to activate this function. The default is *Off*.

9.3.4.5.2 *Time Interval*

In the *Minimum interval* text box, enter the number of seconds for the minimum interval between alarms. The range is from 20 to 3600 seconds.

9.3.4.5.3 *Triggered Action*

The Administrator can specify multiple alarm actions to be taken when a triggering event occurs. The options are listed as follows:

- *Upload Image by FTP* – Selecting this option enables you to assign an FTP site and configure various parameters, as seen in Figure 57: Upload Image by FTP. When the alarm is triggered, event images will be uploaded to the designated FTP site.

> **Note:**
> Images can be sent by FTP only when MJPEG is selected as the video stream from the Video Format screen.

- Specify the FTP address to use from the drop-down menu. Select the number of frames for the pre-trigger and post-trigger buffers from the drop-down menu of 1-20 frames.

- *Upload Image by E-Mail* – Selecting this option enables you to assign an e-mail address and configure various parameters, as shown in Figure 60: Upload Image by E-Mail. When an alarm is triggered, event images will be sent to the designated e-mail address.

> **Note:**
> Images can be sent by e-mail only when MJPEG is selected as the video stream from the Video Format screen.

Select one of two e-mail addresses from the drop-down menu. Select the number of frames for the pre-trigger and post-trigger buffers from the drop-down menu of 1-20 frames.

> **Note:**
> Make sure SMTP or FTP configuration has been completed. See the Mail and FTP sections for further details.

9.3.4.5.4 *File Name*

- *File Name* – Enter a file name in the field, for example *image.jpg.* The uploaded image's file name format is set in this section. Select one that meets your requirements.
- Add date/time suffix (default setting)
  File name: imageYYMMDD_HHNNSS_XX.jpg
  Y: Year, M: Month, D: Day
  H: Hour, N: Minute, S: Second
  X: Sequence Number
- Add sequence number suffix (no maximum value)
  File name: imageXXXXXXX.jpg
  X: Sequence Number
- Add sequence number suffix (limited value)
  File Name: imageXX.jpg
  X: Sequence Number

  The file name suffix ends at the number being set. For example, if the setting is up to "10," the file name will start from 00, end at 10, and then start over again.
- Overwrite
  The original image in the FTP site will be overwritten by the new uploaded file with a static filename.

Click **SAVE** after configuring the settings.

9.3.4.6 Manual Trigger

The **Manual Trigger** screen is used to specify an alarm to be manually triggered. You can define action to take when an alarm occurs from the System > Events Setup > IO screen.

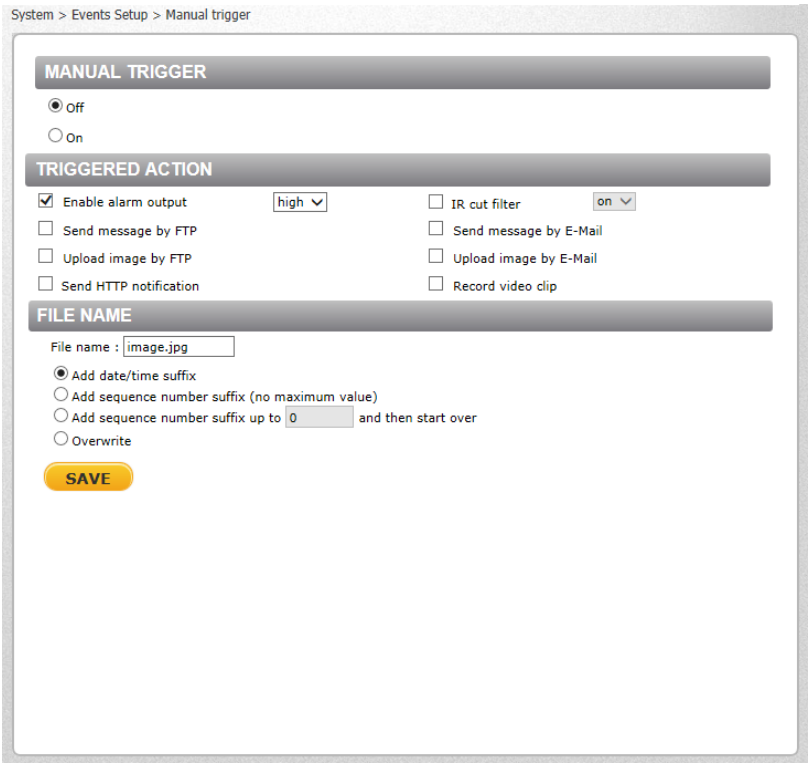


Figure 65: Manual Trigger Screen

9.3.4.6.1 *Manual Trigger*

Select *Off* or *On* to activate this function. The default is *Off*.

9.3.4.6.2 *Triggered Action*

Specify one or both alarms to trigger:

- *Enable alarm output* – Check this box and select the predefined type of alarm output *(high* or *low*) to enable alarm relay when an alarm is triggered.
- *Send Message by FTP* – The Administrator can select whether to send an alarm message by FTP when an alarm is triggered.
- *Upload Image by FTP* – Selecting this option enables you to assign an FTP site and configure various parameters, as seen in Figure 57: Upload Image by FTP. When an alarm is triggered, event images will be uploaded to the designated FTP site.

> **Note:**
> Images can be sent by FTP only when MJPEG is selected as the video stream from the Video Format screen.

Specify the FTP address to use from the drop-down menu. Select the number of frames for the pre-trigger and post-trigger buffers from the drop-down menu of 1-20 frames.

Check the box for *Continue image upload if* you wish to use this option. To specify the length of time for the upload, click this radial button and enter the number of seconds. To upload while the trigger is active, click this radial button.

Finally, select the number of frames per second from the drop-down menu next to *Image frequency*.

- *Send HTTP notification* – Check this option, select the destination HTTP address, and specify the parameters for HTTP notifications. When an alarm is triggered, the HTTP notifications can be sent to the specified HTTP server. See Figure 58: Send HTTP Notification.
- *IR Cut Filter* – Select this checkbox to trigger an event when the IR cut filter is activated. From the drop-down menu, select *on* or *off*. When the IR Cut filter is set to *on,* the IR LED illuminator is activated for use in low-light environments in which Night mode is normally used.
- *Send message by E-Mail* – The Administrator can select whether to send an alarm message by e-mail when an alarm is triggered.
- *Upload Image by E-Mail* – Selecting this option enables you to assign an e-mail address and configure various parameters, as shown in Figure 60: Upload Image by E-Mail. When an alarm is triggered, event images will be sent to the designated e-mail address.

> **Note:**
> Images can be sent by e-mail only when MJPEG is selected as the video stream from the Video Format screen.

Select one of two e-mail addresses from the drop-down menu. Select the number of frames for the pre-trigger and post-trigger buffers from the drop-down menu of 1-20 frames.

Check the box for *Continue image upload* if you wish to use this option. To specify the length of time for the upload, click this radial button and enter the number of seconds. To upload during the active trigger, click this radial button. Finally, select the number of frames per second from the drop-down menu next to *Image frequency.*

> **Note:**
> Make sure SMTP or FTP configuration has been completed. See the Mail and FTP sections for further details.

- *Record video clip* – Select this box in order to save the alarm-triggered recording into a microSDXC card. Enter the number of seconds for the pre-trigger buffer. Select the first radial button to upload for a specified length of time and enter the number of seconds. Alternatively, select the second radial button to upload during the active trigger. See Figure 59: Record Video Clip.

> **Note:**
> To implement function, make sure that local recording with a microSDXC card is activated and that the NAS is properly configured. See Recording for details.

9.3.4.6.3 *File Name*

- *File Name* – Enter a file name in the field, for example *image.jpg.* The uploaded image's file name format is set in this section. Select one that meets your requirements.
- Add date/time suffix (default setting)
  File name: imageYYMMDD_HHNNSS_XX.jpg
  Y: Year, M: Month, D: Day
  H: Hour, N: Minute, S: Second
  X: Sequence Number

- Add sequence number suffix (no maximum value)
  File name: imageXXXXXXX.jpg
  X: Sequence Number
- Add sequence number suffix (limited value)
  File Name: imageXX.jpg
  X: Sequence Number

  The file name suffix ends at the number being set. For example, if the setting is up to "10," the file name will start from 00, end at 10, and then start over again.
- Overwrite
  The original image in the FTP site will be overwritten by the new uploaded file with a static filename.

Click **SAVE** after configuring the settings

9.3.5 Edge Recording

From the **Edge Recording** tab it is possible to configure the following screens:

- SD Card
- Network Share
- Recording

9.3.5.1 SD Card

You can locally record up to 128GB on a Class 10 microSDXC card. The **SD Card** page shows the capacity information of the memory card and a recording list of all the recording files saved on the card. You can also format the card and implement automatic recording cleanup on this page. To implement microSDXC card recording, see Recording.

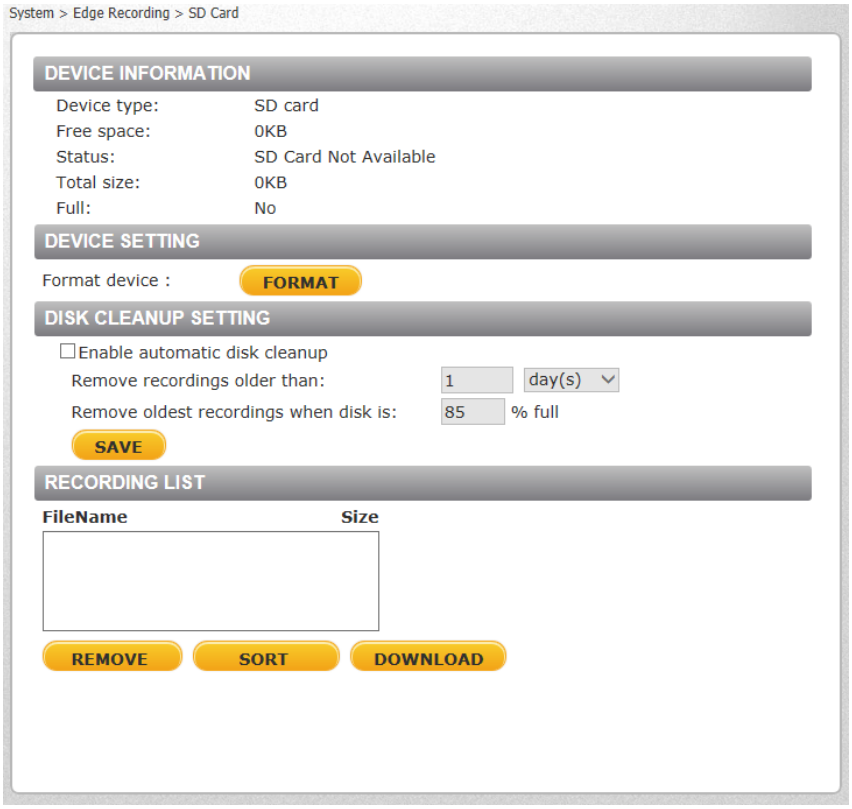


Figure 66: SD Card Screen

Note:
Format the microSDXC card when using it for the first time. Formatting is also required when a memory card has been used on one camera and is then transferred to a camera that uses a different software platform.

Device Information

Upon inserting the microSDXC card, card information, such as the memory capacity and status, is displayed.

Device Setting

Click **Format** to format the memory card.

Disk Cleanup Setting

Enable automatic recording cleanup by selecting *Enable automatic disk cleanup*. From the pull-down menu, specify the minimum length of time over which to remove recordings. For example, remove recordings over 10 days old. Enter the percent of disk capacity used in order to remove the oldest recordings. Click **SAVE** when finished.

Recording List

Each video file on the microSDXC card is listed in the Recording List table below. The maximum file size is 60 MB per file. See Recording for further details.

When the recording mode in the **Recording** screen is set as *Always* (consecutive recording) and the microSDXC card recording is enabled by events triggered, the system immediately saves a recorded event on the memory card once an event occurs. The camera then returns to the regular recording mode after events recording.

Figure 67: Video File Recording List

- *Remove* – To remove a file, first select the file and then click **REMOVE**.
- *Sort* – Click **SORT** to list the files in the Recording List table in order of name and date.

Note:
The capital letters: R, N, A, (A0), M, (M0) followed by an underscore, appear at the beginning of the file name. They denote the type of recording.

- R - Regular (always or schedule)
- N - Network failure
- M - Motion, (M0 refers to the first motion window trigger)
- A - Alarm (A0 refers to the first alarm trigger input).

- *Download* – To open/download a video clip, first select the file and then click **DOWNLOAD**. The selected file window pops up as shown below. Click the AVI file to play the video in the player or download it to a specified location.

Figure 68: Selected File Window

9.3.5.2 Network Share

The **Network Share** screen shows the capacity information of the Network Attached Storage (NAS) disk and provides a list of all the recording files saved on the disk.

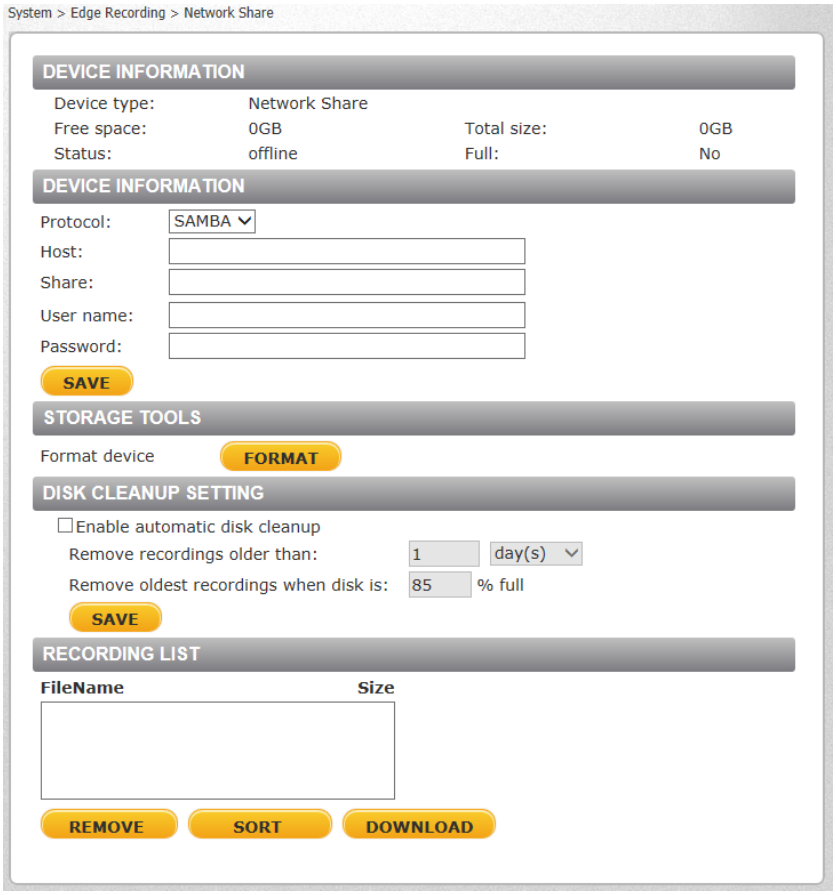


Figure 69: Network Share Screen

You can also format the disk and implement automatic recording cleanup on this page. To implement NAS recording, see Recording.

Device Information

Upon connecting to the NAS, the following information about the disk is displayed:

- *Device type* – Displays *Network Share*
- *Free space* – Displays the amount of available storage space in GB
- *Total size* – Displays the total amount of storage space in GB
- *Status* – Indicates if the camera is online or offline
- *Full* – Indicates if the disk is full (Yes/No)
- *Protocol* – Displays the protocol used by the NAS. The default is SAMBA.

Enter the details for the following fields:

- *Host* – Enter the host IP address
- *Share* – Enter the path for a shared network storage device
- *User name* – Enter the name of the user accessing the NAS
- *Password* – Enter the password of the user accessing the NAS

Storage Tools

Click **FORMAT** to format the NAS.

Disk Cleanup Setting

Enable automatic recording cleanup by selecting *Enable automatic disk cleanup*. From the pull-down menu, specify the minimum length of time over which to remove recordings. For example, remove recordings over 10 days old. Enter the percent of disk capacity used in order to remove the oldest recordings. Click **SAVE** when finished.

Recording List

Each video file stored on the NAS is listed in the Recording list. See Recording for further details. When the recording mode in the Recording screen is set as *Always* (consecutive recording) and the NAS recording is enabled by events triggered, the system immediately saves a recorded event on the network disk once an event occurs. Then the camera will return to the regular recording mode after events recording.

Figure 70: Video File Recording List

- *Remove* – To remove a file, first select the file and then click **REMOVE**.
- *Sort* – Click **SORT** to list the files in the Recording list in order of name and date.

Note:
The capital letters: R, N, A, (A0), M, (M0) followed by an underscore, appear at the beginning of the file name. They denote the type of recording.

- R - Regular (always or schedule)
- N - Network failure
- M - Motion, (M0 refers to the first motion window trigger)
- A - Alarm (A0 refers to the first alarm trigger input).

- *Download* – To open/download a video clip, first select the file and then click **DOWNLOAD**. The selected file window pops up as shown below. Click the AVI file to play the video in the player or download it to a specified location.

Figure 71: Selected File Window

9.3.5.3 Recording

The **Recording** screen is used to select a device and to set a schedule for recording clips. Up to 10 schedules can be set.

In the *Recording Storage* section, select the recording device: *SD Card* or *Network Share*.

Note:

It is not recommend to record with the microSD card for 24/7 continuously, as it may not be able to support long term continuous data read/write. Contact the manufacturer of the microSD card for information regarding its reliability and life expectancy.

In the *Recording Schedule* section, specify the recording schedule. Select one of three options:

- *Disable* – Disable this function
- *Always* – Always use this function
- *Only during time frame* – Records only during a specified time frame

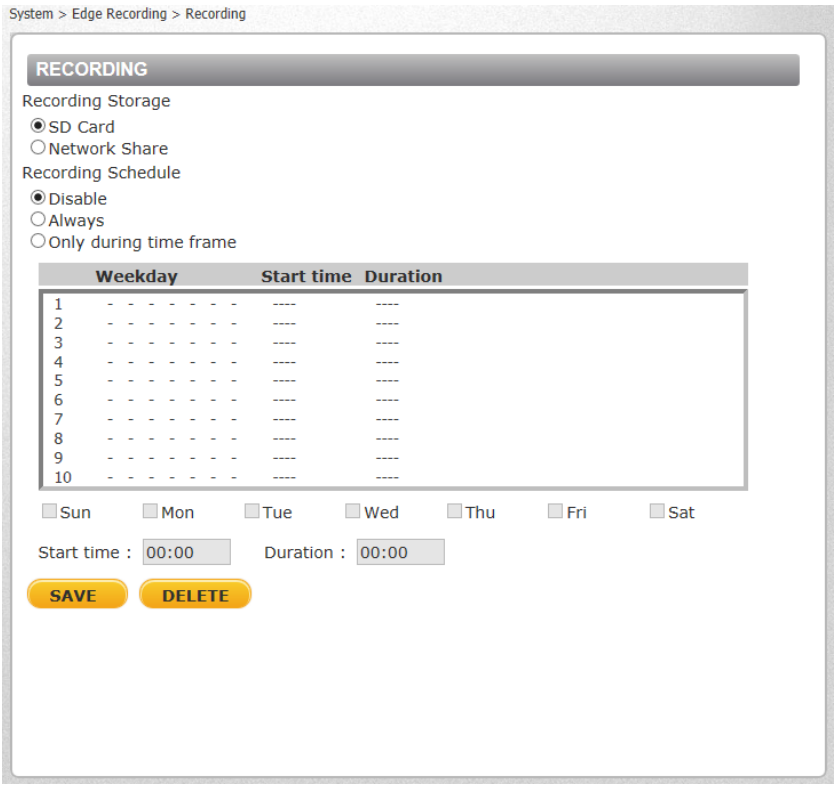


Figure 72: Recording Screen

To set the recording schedule

1. Selecting the day.
2. Set the start time.
3. Set the duration for recording.
4. Click **SAVE** to confirm the schedule. The schedule is displayed in the table.

> **Note:**
> This option works only if (a) the microSDXC card is installed in the camera or (b) the NAS is configured properly.

9.3.6 Motion Detection

The motion detection function detects suspicious motion and triggers alarms when motion volume in the detected area reaches or exceeds the determined sensitivity threshold value.

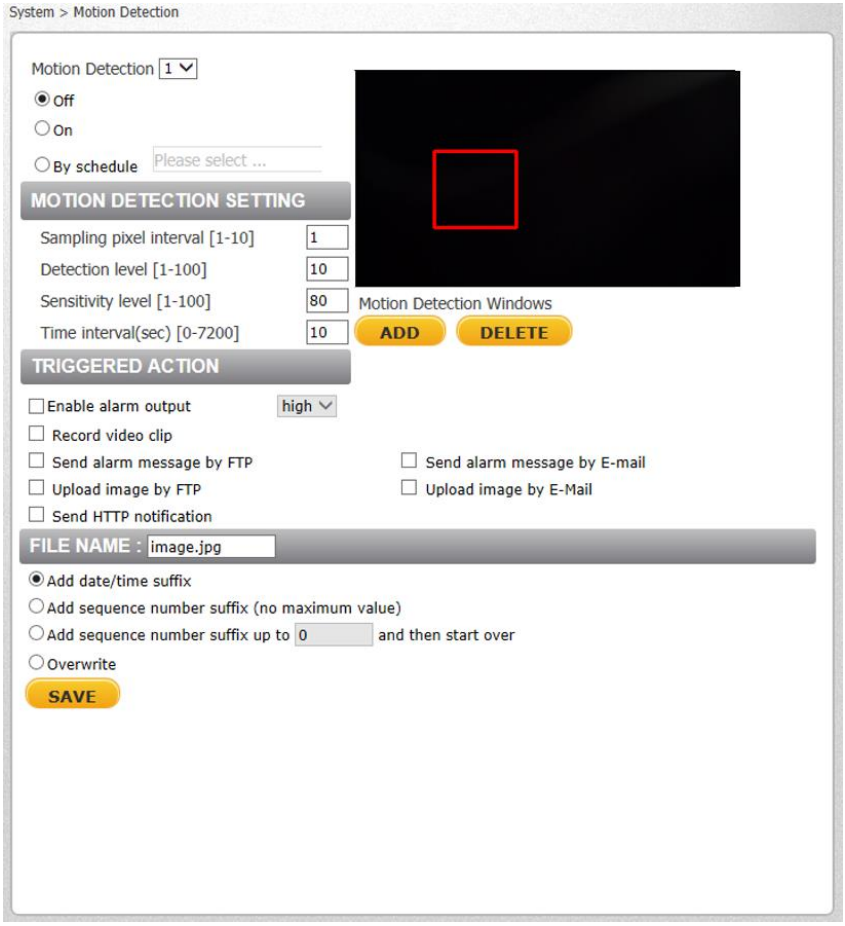


Figure 73: Motion Detection Screen

Within the Live View pane on the **Motion Detection** screen, there is a frame (**Motion Detection** window) which is used for defining the motion detection area. To change the size of the **Motion Detection** window, move the mouse cursor to the edge of the frame and drag it outward or inward. Moving the mouse to the center of the frame shifts the frame to the intended location.

Motion Detection Activation

It is possible to define up to four motion detection zones within the **Motion Detection** window by selecting a number from the drop-down menu.

The motion detection function may be turned on or off in the *Motion Detection* section of the screen. The default setting is *Off.* Alternatively, you may select *By schedule* to set a schedule.

To set a schedule

1. Select *By schedule*. The message *Please Select* is displayed.
2. Click *Please select*. A drop-down menu opens.
3. From the drop-down menu, select a schedule from 1 to 10. The selected schedules are displayed in a horizontal field above the drop-down menu.

For instructions how to set a schedule for motion detection, refer to Schedule. Below is a screen showing the *Schedule* drop-down menu with selected schedules.

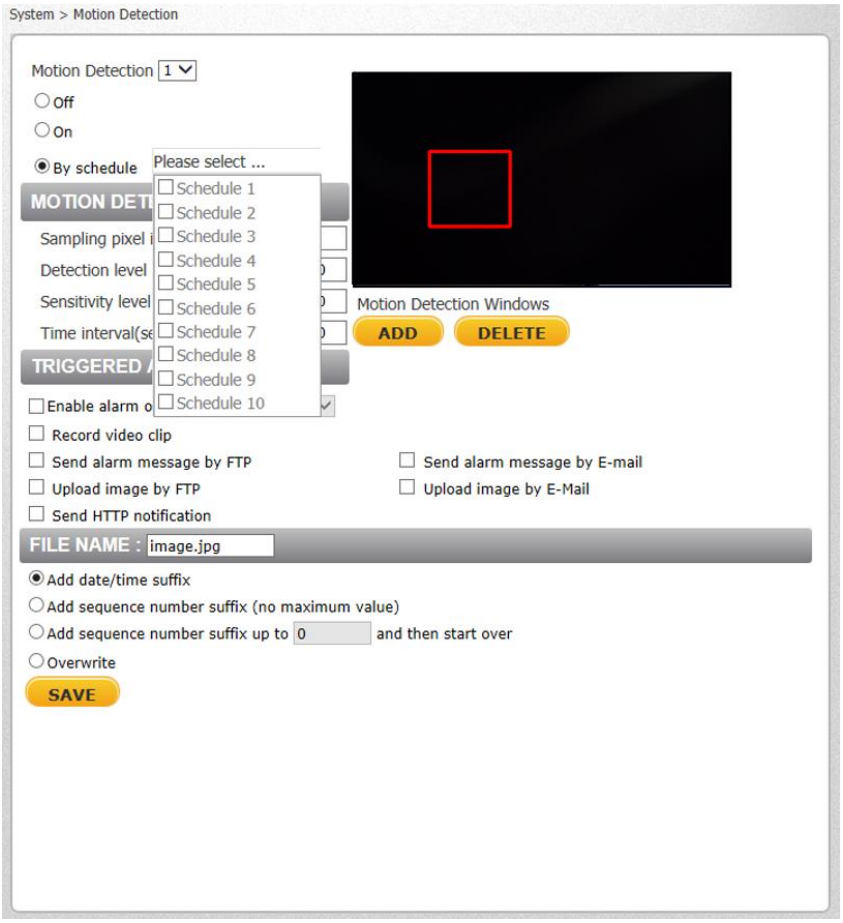


Figure 74: Motion Detection Screen – with Schedule Drop-Down Menu

Motion Detection Windows

Up to 10 **Motion Detection** windows can be set. Click the **ADD** button under the Live View pane to add a **Motion Detection** window. To cancel a **Motion Detection** window, move the mouse cursor to the selected window and click **DELETE**.

If the motion detection function is activated, the following **Motion** pop-up window appears.

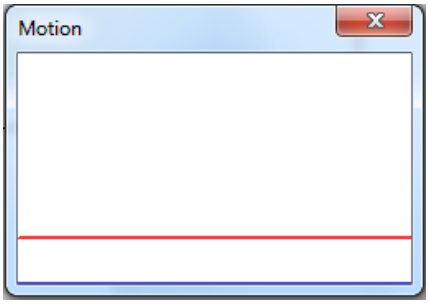


Figure 75: Motion Window without Detection

When motion is detected, the signals are displayed in the **Motion** window shown below.

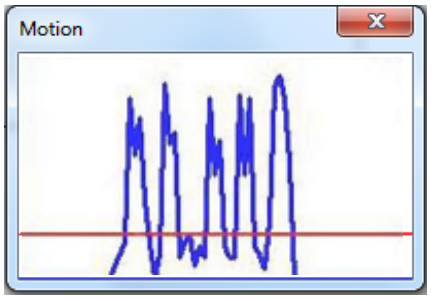


Figure 76: Motion Window with Detection

Detailed settings for motion detection are as follows:

- *Sampling pixel interval* [*1-10]* – Select a number from 1-10. The default value is 1. If the value is set as 3, within the detection region, the system will take one sampling pixel for every 3 pixels by each row and each column (see the figure below).

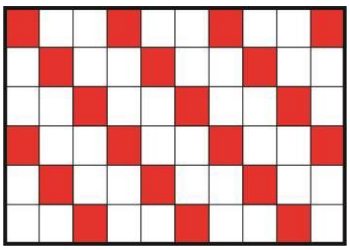


Figure 77: Pixel Interval Illustration

- *Detection level* [*1-100]* – Select a number from 1-100. The default level is 40. This sets detection level for each sampling pixel; the smaller the value, the more sensitive it is.
- *Sensitivity level [1-100]* – Select a number from 1-100. The default level is 80, which means if 20% or more sampling pixels are detected differently, the system will detect motion. The bigger the value, the more sensitive it is. When the value is bigger, the red horizontal line in the motion indication window will be lowered accordingly.
- *Time interval (sec) [0-7200]* – Select a number from 0-7200 (seconds). The default interval is 10. The value is the interval between each detected motion.

Triggered Action

The Administrator can specify alarm actions to be taken when motion is detected. See Figure 73: Motion Detection Screen. The options are listed as follows:

- *Enable alarm output* – Check this box and select the predefined type of alarm output *(low* or *high*) to enable alarm relay when tampering is detected.
- *Record video clip* – Select this box to store the motion detection alarm recording in a microSDXC card or on the NAS when tampering is detected. Enter the number of seconds for the pre-trigger buffer. Select the first radial button to upload for a specified length of time and enter the number of seconds. Alternatively, select the second radial button to upload during the active trigger.

> **Note:**
> Make sure the local recording (with microSDXC card) is activated so that this function can be implemented. See Recording for further details.

- *Send alarm message by FTP* – Select whether to send an alarm message by FTP when motion is detected.

- *Upload image by FTP* – Select this box in order to upload an image to a designated FTP site when motion is detected according to various parameters, as seen in Figure 57: Upload Image by FTP.

  Note:
  Images can be sent by FTP only when MJPEG is selected as the video stream from the Video Format screen.

  Specify the FTP address to use from the drop-down menu. Select the number of frames for the pre-trigger and post-trigger buffers from the drop-down menu of 1-20 frames.

  Check the box for *Continue image upload* if you wish to use this option. To specify the length of time for the upload, click this radial button and enter the number of seconds. To upload while the trigger is active, click this radial button. Finally, select the number of frames per second from the drop-down menu next to *Image frequency*.

- *Send HTTP notification* – Check this box to send a notification by HTTP. Select the destination HTTP address from the drop-down menu and specify the parameters for event notifications by motion detection triggered. When an alarm is triggered, the notification will be sent to one of two specified HTTP servers. See Figure 58: Send HTTP Notification.

- *Send alarm message by E-Mail* – Select whether to send an alarm message by e-mail when motion is detected.

  Note:
  Make sure that local recording (with a microSDXC card) is activated so that this function can be implemented. See Recording for further details.

- *Upload image by E-Mail* – Select this box in order to assign an e-mail address and configure various parameters, as seen in Figure 60: Upload Image by E-Mail.

  Note:
  Images can be sent by e-mail only when MJPEG is selected as the video stream from the Video Format screen.

  When motion is detected, event images are sent to one of two designated e-mail addresses. Select the number of frames for the pre-trigger and post-trigger buffers from the drop-down menu of 1-20 frames.

  Check the box for *Continue image upload* to use this option. To specify the length of time for the upload, click this radial button and enter the number of seconds. To upload while the trigger is active, click this radial button. Finally, select the number of frames per second from the drop-down menu next to *Image frequency.*

  Note:
  Make sure that SMTP or FTP configuration has been completed. See the Mail and FTP sections for further details.

File Name

The uploaded image's filename format is set in this section. Select one that meets your requirements.

Save

Click **SAVE** to save the motion detection settings.

9.3.7 Schedule

The **Schedule** screen is used by the network failure detection, tampering and motion detection functions. To access the schedule function, open the **Main** window, select the **System** tab, and click the **Schedule** tab. The functions in this tab allow administrators to create customized schedules for the camera. If a schedule exists, the administrator can apply that schedule to this camera using the available dropdown. See Figure 78: Schedule Screen.

Note:
This application is not the same as the Recording Schedule function.

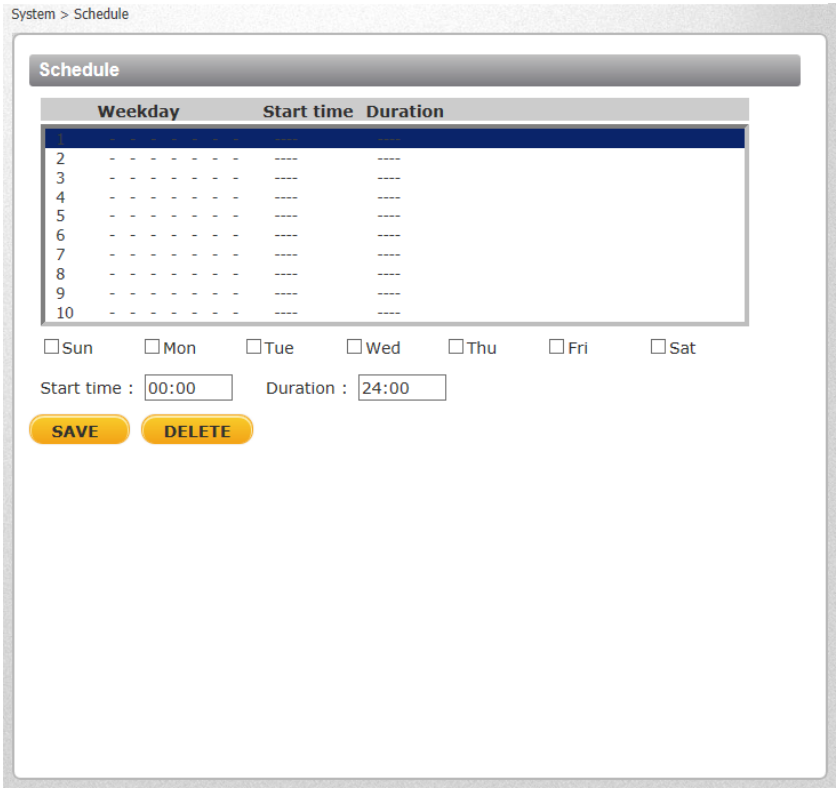

System > Schedule
Schedule
Weekday
Start time
Duration
1 - - - - - - - ---- ----
2 - - - - - - - ---- ----
3 - - - - - - - ---- ----
4 - - - - - - - ---- ----
5 - - - - - - - ---- ----
6 - - - - - - - ---- ----
7 - - - - - - - ---- ----
8 - - - - - - - ---- ----
9 - - - - - - - ---- ----
10 - - - - - - - ---- ----
Sun
Mon
Tue
Wed
Thu
Fri
Sat
Start time : 00:00
Duration : 24:00
SAVE
DELETE

Figure 78: Schedule Screen

To create a new schedule or edit an existing schedule

1. Select the appropriate checkbox for the day(s) of the week (Sun, Mon, Tue, Wed, Thu, Fri and Sat) to create a schedule.
   See Figure 78.
2. Set Start time (for example, 09:00) and Duration (for example, 4:00 hours).
3. Click **SAVE** to apply the newly created schedule to the camera.

To remove a schedule

1. To remove a schedule, select the setup data line by line.
2. Click **DELETE** to remove.

9.3.8 File Location

From the **File Location** page, specify a storage location for snapshots and web recordings. The default setting is: C:\. After confirming the setting, click **SAVE** to save the snapshots and recordings in the designated location.

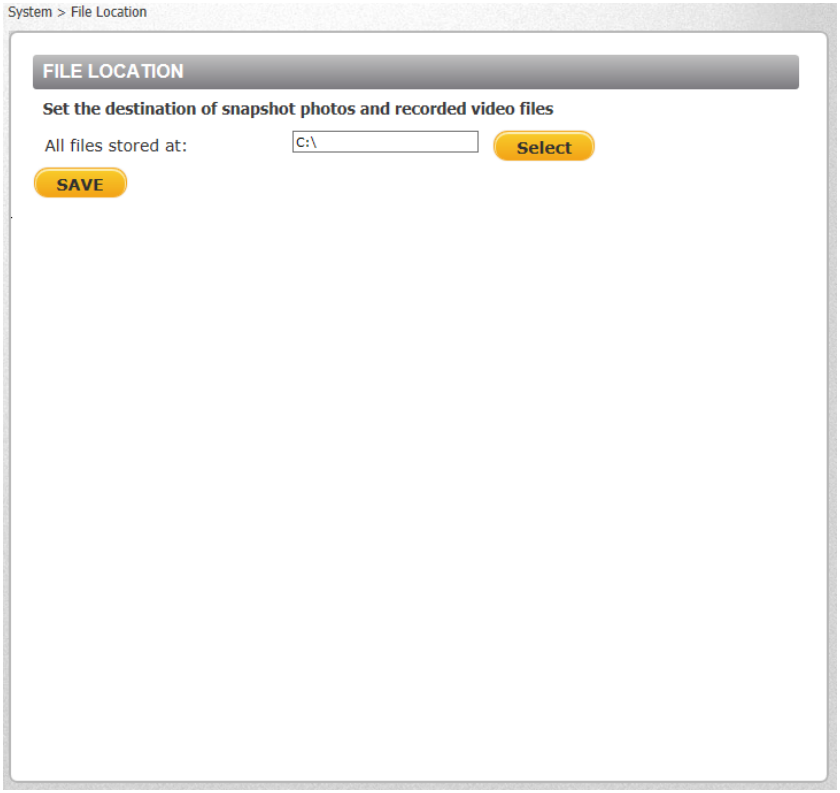


Figure 79: File Location Screen

Note:
Make sure the selected file path contains valid characters.

9.3.9 Maintenance

Clicking the **Maintenance** tab in the **System** screen opens a drop-down menu with the following tabs:

- Log File
- User Information
- Factory Default
- Software Version
- Software Upgrade
- Parameters

9.3.9.1 Log File

Click **Log file** to view the system log file. The content of the file provides information about connections after system boot-up.

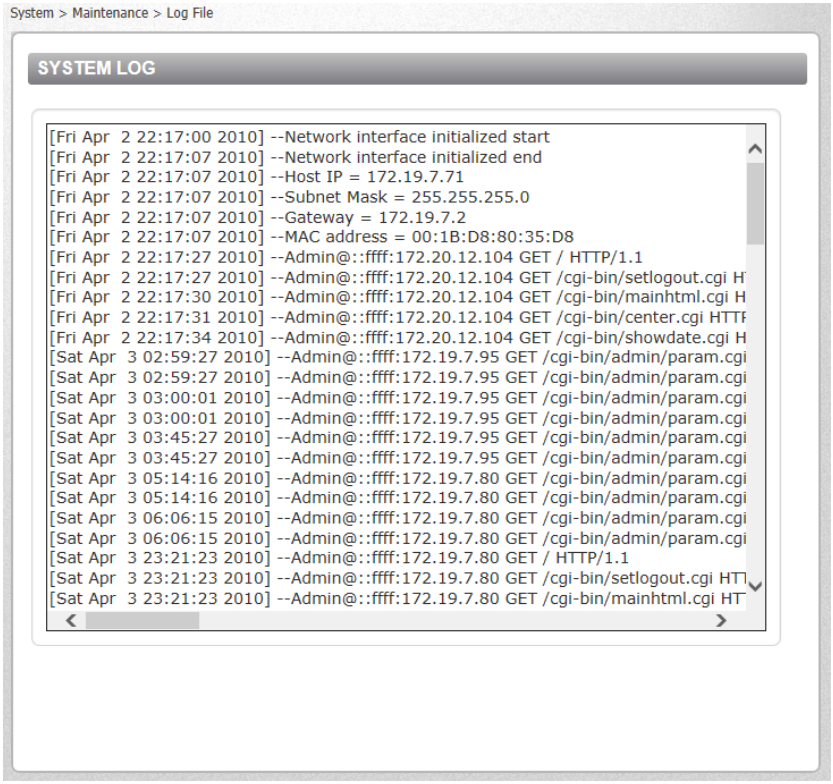

System > Maintenance > Log File
SYSTEM LOG
[Fri Apr 2 22:17:00 2010] --Network interface initialized start
[Fri Apr 2 22:17:07 2010] --Network interface initialized end
[Fri Apr 2 22:17:07 2010] --Host IP = 172.19.7.71
[Fri Apr 2 22:17:07 2010] --Subnet Mask = 255.255.255.0
[Fri Apr 2 22:17:07 2010] --Gateway = 172.19.7.2
[Fri Apr 2 22:17:07 2010] --MAC address = 00:1B:D8:80:35:D8
[Fri Apr 2 22:17:27 2010] --Admin@::ffff:172.20.12.104 GET / HTTP/1.1
[Fri Apr 2 22:17:27 2010] --Admin@::ffff:172.20.12.104 GET /cgi-bin/setlogout.cgi H
[Fri Apr 2 22:17:30 2010] --Admin@::ffff:172.20.12.104 GET /cgi-bin/mainhtml.cgi H
[Fri Apr 2 22:17:31 2010] --Admin@::ffff:172.20.12.104 GET /cgi-bin/center.cgi HTTP
[Fri Apr 2 22:17:34 2010] --Admin@::ffff:172.20.12.104 GET /cgi-bin/showdate.cgi H
[Sat Apr 3 02:59:27 2010] --Admin@::ffff:172.19.7.95 GET /cgi-bin/admin/param.cgi
[Sat Apr 3 02:59:27 2010] --Admin@::ffff:172.19.7.95 GET /cgi-bin/admin/param.cgi
[Sat Apr 3 03:00:01 2010] --Admin@::ffff:172.19.7.95 GET /cgi-bin/admin/param.cgi
[Sat Apr 3 03:00:01 2010] --Admin@::ffff:172.19.7.95 GET /cgi-bin/admin/param.cgi
[Sat Apr 3 03:45:27 2010] --Admin@::ffff:172.19.7.95 GET /cgi-bin/admin/param.cgi
[Sat Apr 3 03:45:27 2010] --Admin@::ffff:172.19.7.95 GET /cgi-bin/admin/param.cgi
[Sat Apr 3 05:14:16 2010] --Admin@::ffff:172.19.7.80 GET /cgi-bin/admin/param.cgi
[Sat Apr 3 05:14:16 2010] --Admin@::ffff:172.19.7.80 GET /cgi-bin/admin/param.cgi
[Sat Apr 3 06:06:15 2010] --Admin@::ffff:172.19.7.80 GET /cgi-bin/admin/param.cgi
[Sat Apr 3 06:06:15 2010] --Admin@::ffff:172.19.7.80 GET /cgi-bin/admin/param.cgi
[Sat Apr 3 23:21:23 2010] --Admin@::ffff:172.19.7.80 GET / HTTP/1.1
[Sat Apr 3 23:21:23 2010] --Admin@::ffff:172.19.7.80 GET /cgi-bin/setlogout.cgi HT
[Sat Apr 3 23:21:23 2010] --Admin@::ffff:172.19.7.80 GET /cgi-bin/mainhtml.cgi HT

Figure 80: Log File Screen

9.3.9.2 User Information

The Administrator can view each user's login information and privileges in the **User information** screen shown below.

Note:

User credentials and privileges are set in the User screen (page 33).

View User Login Information

Click **GET USER INFORMATION** to see each user's details. For example: *Admin: 1234*. This indicates that the user's login username is *Admin* and the password is *1234*.

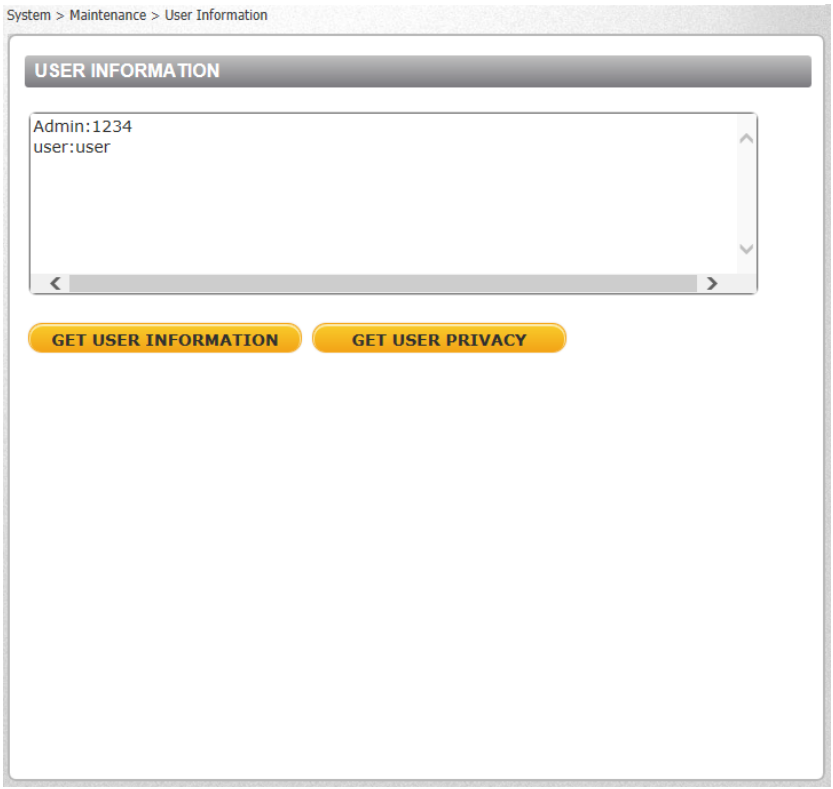


Figure 81: User Information Screen – Get User Information

View User Privilege

Click **GET USER PRIVACY** to view each user's privileges.

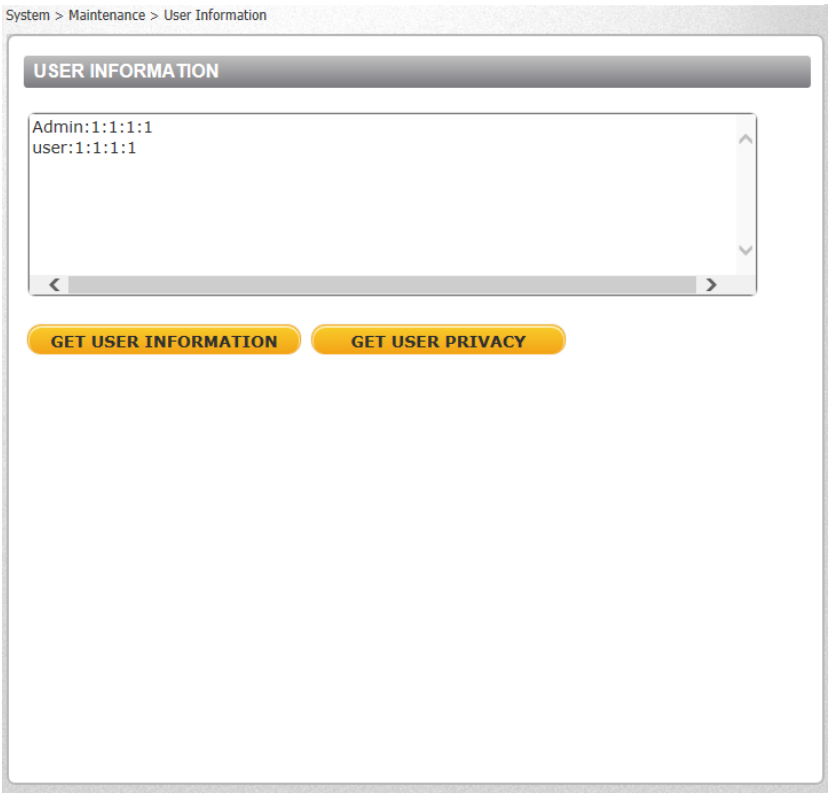
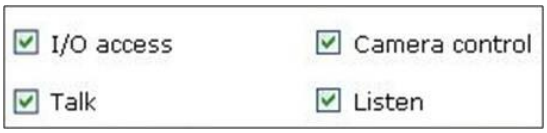


Figure 82: User Information – Get User Privacy

In the screen above, both *Admin* and *User* are granted privileges of I/O access, Camera control, Talk and Listen, which are the maximum privileges that can be granted.



9.3.9.3 Factory Default

The **Factory default** page is shown below. Follow the instructions to reset the camera to factory default settings if needed.

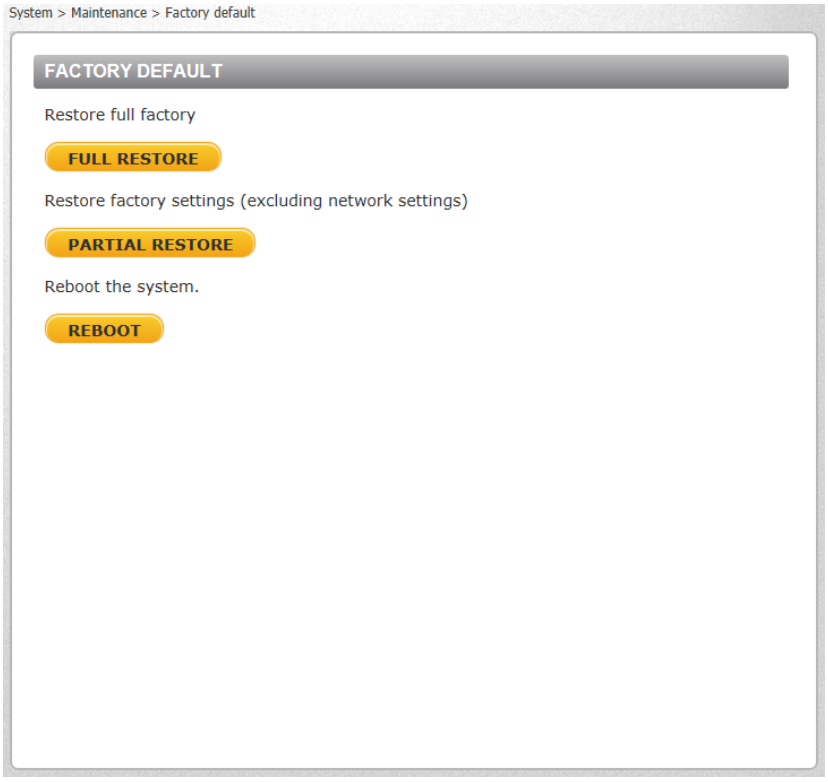


Figure 83: Factory Default Screen

Full Restore

Click **FULL RESTORE** to restore the factory default settings. The system restarts in 30 seconds.

Note:
The IP address and all other settings will be restored to factory default settings.

Partial Restore

Click **PARTIAL RESTORE** to restore the factory default settings, but save the network settings. The system restarts in 30 seconds.

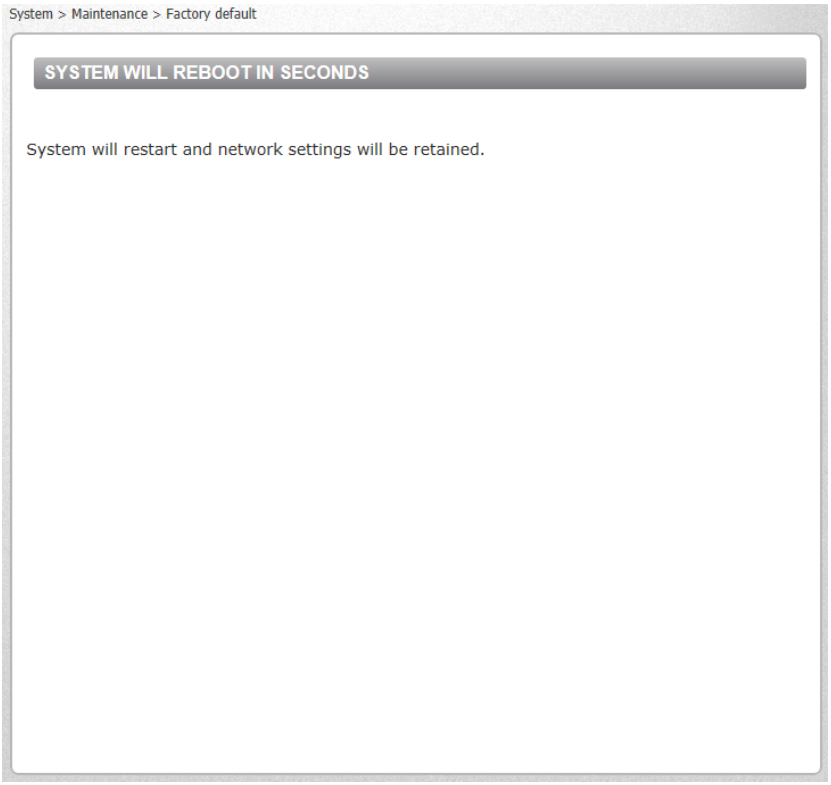

System > Maintenance > Factory default
SYSTEM WILL REBOOT IN SECONDS
System will restart and network settings will be retained.

Figure 84: Partial Restore Screen

Reboot

Click **REBOOT** to restart the system without changing current settings.

9.3.9.4 Software Version

The current version of the software is displayed in the **Software Version** screen.

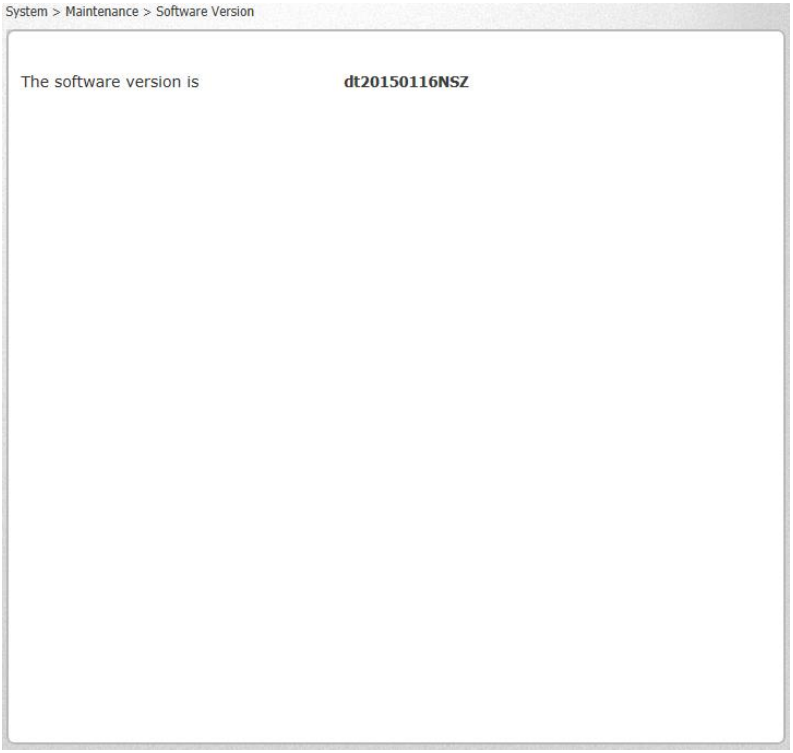


Figure 85: Software Version Screen

9.3.9.5 Software Upgrade

The **Software Upgrade** screen enables you to select a software file to upload.

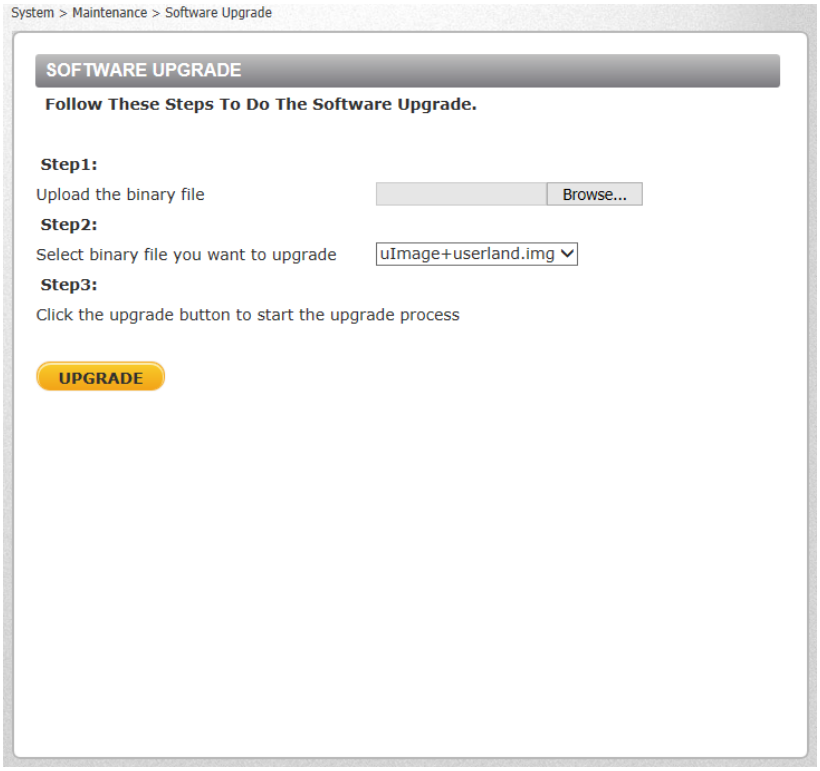


Figure 86: Upgrade Screen

Note:
Make sure that the software upgrade file is available before performing a software upgrade.

To upgrade the software

1. In the *Step 1* text box, click **Browse** and select the binary file to be uploaded, for example, `uImage+userland.img`.

   Note:
   Do not change the file name. If you change the upgrade file name, the system will fail to find the file.

2. From the drop-down menu of binary files in Step 2, select the file to upgrade. In the above example `uImage+userland.img` is selected.
3. Click **UPGRADE**. The system verifies that the upgrade file exists and begins to upload the file. The upgrade status bar is displayed on the page. When the upgrade process is completed, the **Live** page is displayed.

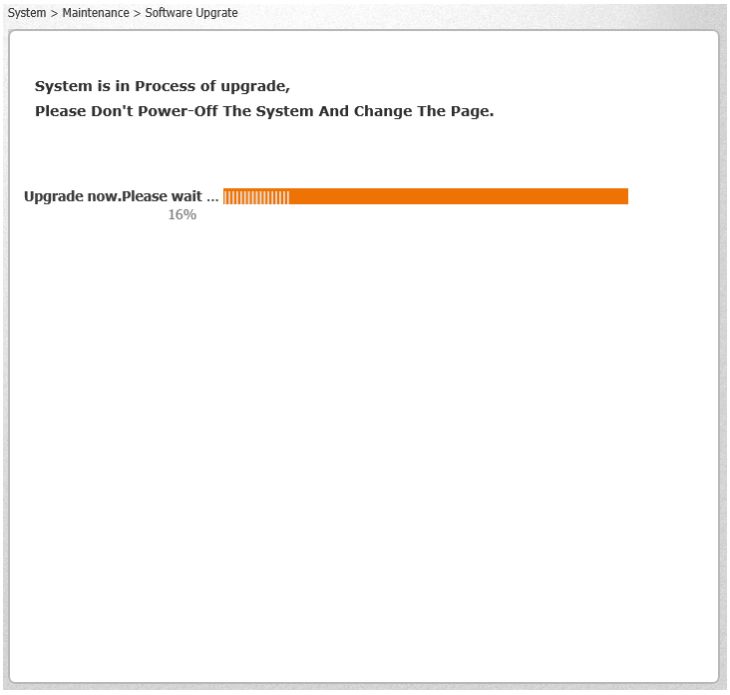

System > Maintenance > Software Upgrate
System is in Process of upgrade,
Please Don't Power-Off The System And Change The Page.
Upgrade now.Please wait ...
16%

Figure 87: Software Upgrade – In Process

4. Close the video browser.
5. From the Windows Start menu, select *Control Panel*.
6. Select *Uninstall a Program.*
7. In the *Currently installed programs* list, select *DVPlayer.*
8. Click **Uninstall** to delete the existing DVPlayer.
9. Install the new DVPlayer ActiveX plug-in.

Warning:
Do not unplug power while upgrading the software.

Avertissement:
Ne débranchez pas l'alimentation pendant la mise à niveau du logiciel.

9.3.9.6 Parameters

The **Parameters** screen displays all of the system's parameter settings.

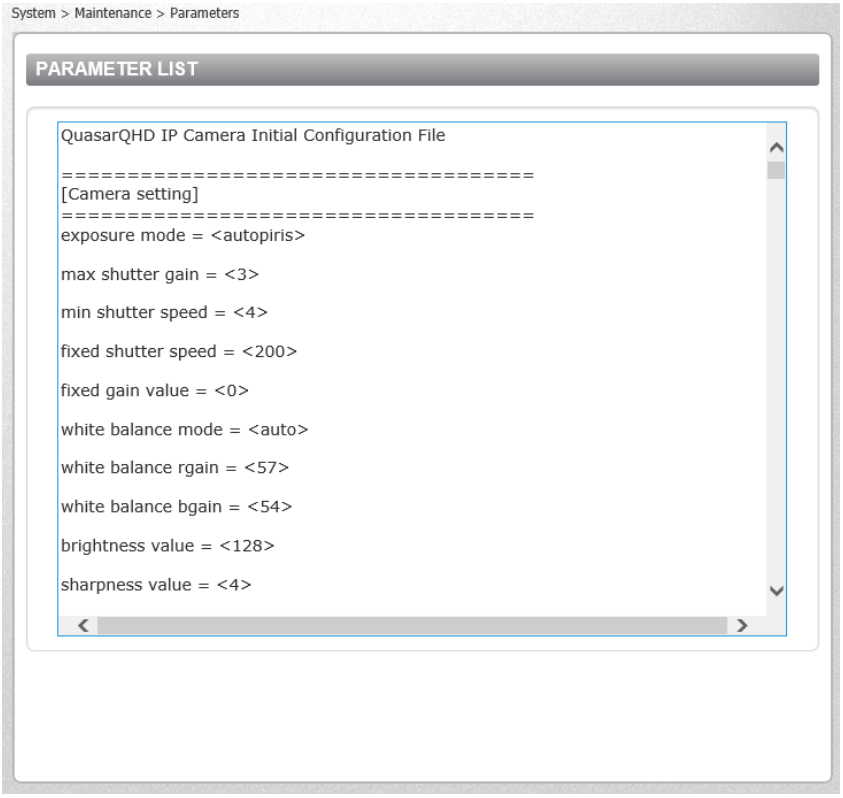


Figure 88: Parameter Screen

Note:
Slide the sidebar located on the right of the screen to view the entire list of parameters.

9.3.10 Import/Export

From the **Import/Export** screen you can export configuration files to a specified location and retrieve data by uploading an existing configuration file to the camera.

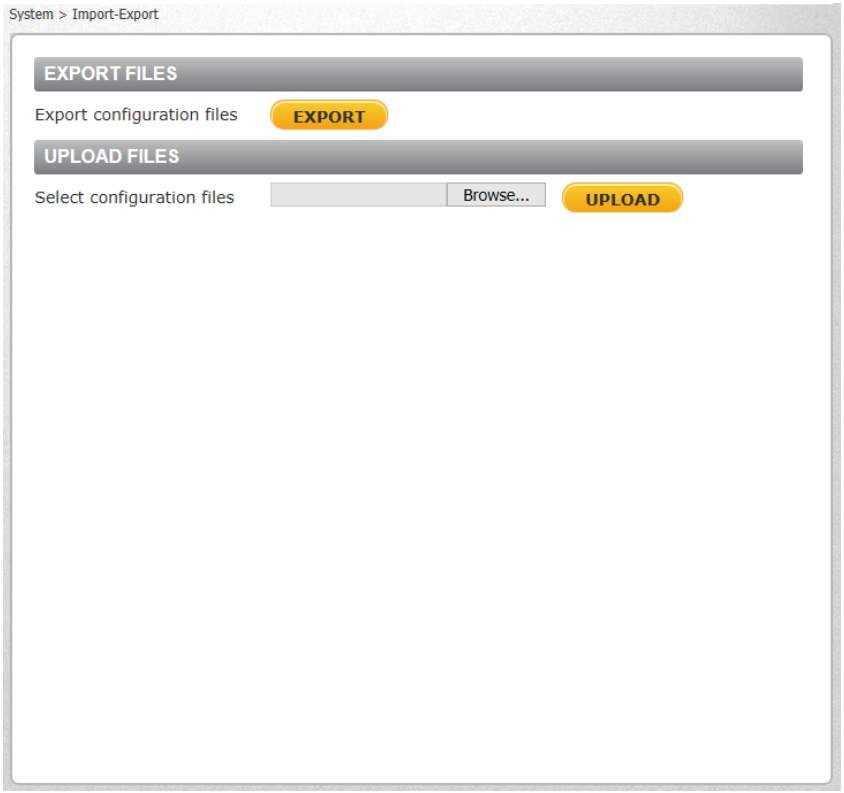


Figure 89: Import/Export Screen

Export

You can save system settings by exporting the configuration file (`.bin`) to a specified location for future use. Click **EXPORT** and the popup window **File Download** appears as shown below.

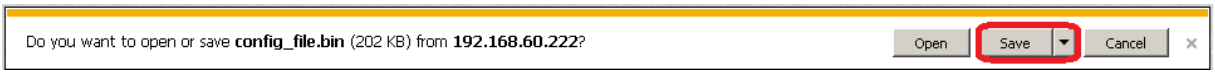


Figure 90: File Download Screen

Click **Save** and specify a location to save the configuration file.

Warning:
Do not unplug power while changing file names.

Avertissement:
Ne débranchez pas l'alimentation pendant la modification des noms de fichiers.

Upload

To copy an existing configuration file to the camera, click **Browse** to select the configuration file, and then click **UPLOAD** to upload the file.

Warning:
Do not unplug power while changing file names.

Avertissement:
Ne débranchez pas l'alimentation pendant la modification des noms de fichiers.

9.4 Streaming Settings

Select the **Streaming** tab in the navigation bar at the top of the page to display the configurable video and audio selections in the sidebar. From the **Streaming** sidebar, the Administrator can configure a specific video resolution, video compression mode, video protocol, audio transmission mode, etc. Details of these settings are specified in the following sections.

- Video Format
- Video Compression
- Video ROI Encoding
- Video OCX Protocol
- Video Frame Rate
- Video Mask
- Audio

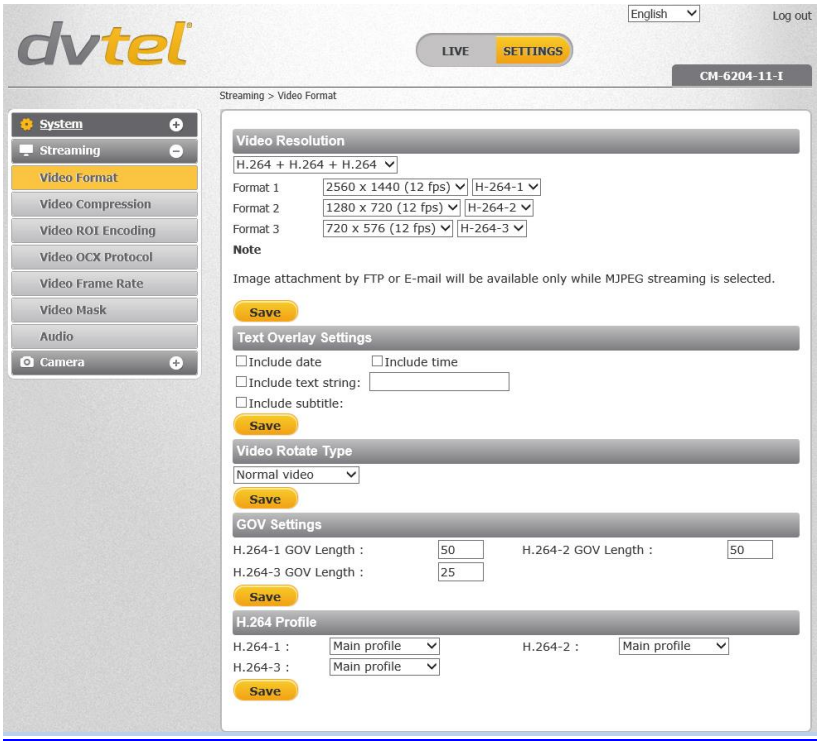


Figure 91: Streaming Section Tabs

9.4.1 Video Format

From the **Video Format** screen, you can configure the following settings:

- Video Resolution Settings
- Text Overlay Settings
- Video Rotate Type
- GOV Settings
- H.264 Profile

CM-6204 cameras support three video streams.

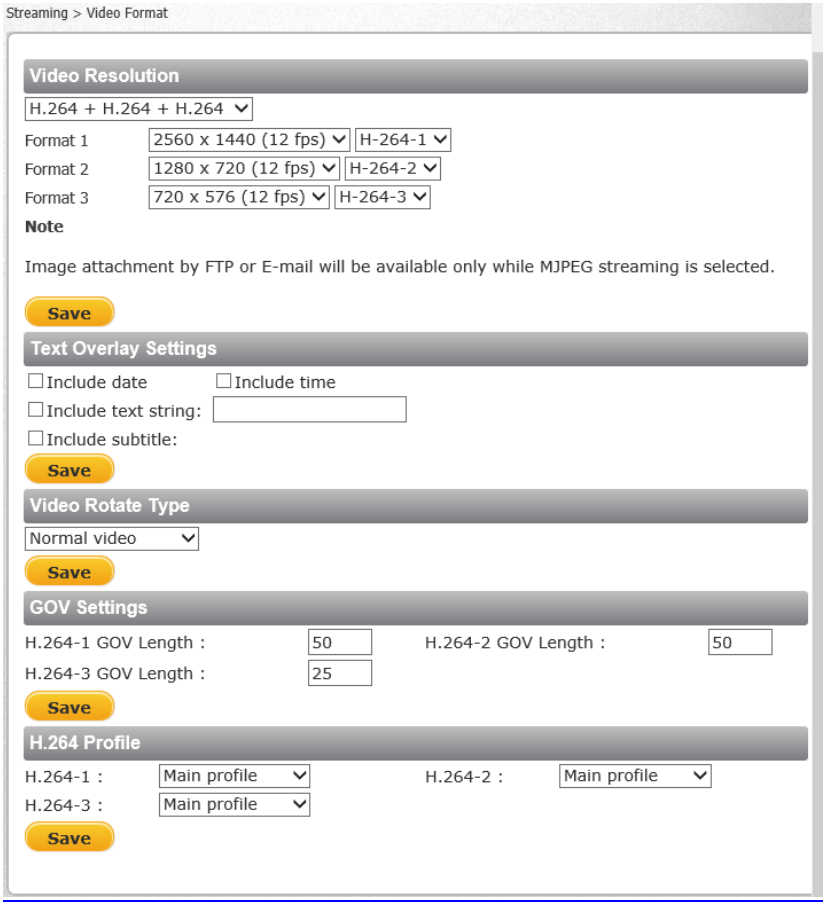


Figure 92: CM-6204 Video Format Screen

CM-6208 cameras support four video streams.

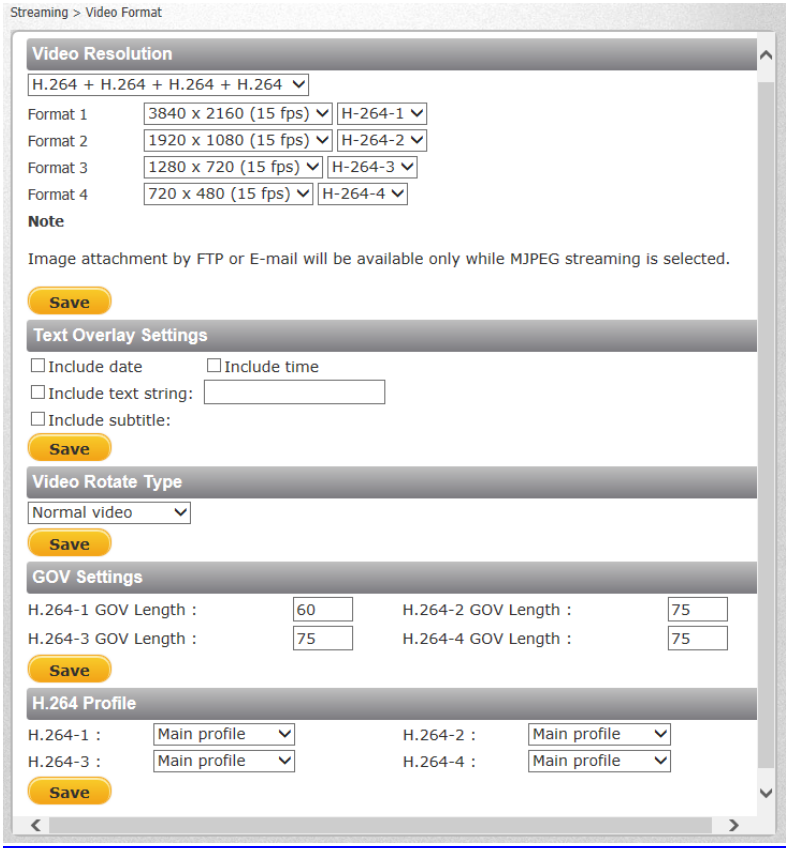


Figure 93: CM-6208 Video Format Screen

9.4.1.1 CM-6204 Video Resolution Settings

The following video resolutions are supported:

- H.264-Only
- MJPEG-Only
- H.264 + H.264 and H.264 + MJPEG
- H.264 + H.264 + H.264 and H.264 + H.264 + MJPEG

9.4.1.1.1 *H.264-Only*

H.264-Only		
TV System	**Stream 1**	**BNC Support**
WDR3	2560 x 1440 (12/15 fps)	Y
WDR2	2560 x 1440 (25/30 fps)	Y
WDR2/3	1280 x 720 (25/30 fps)	Y
WDR2/3	720 x 576 (25 fps) 720 x 480 (30 fps)	Y

9.4.1.1.2 *MJPEG-Only*

MJPEG-Only		
TV System	**Stream 1**	**BNC Support**
WDR2/3	1920 x 1080 (25/30 fps)	Y
WDR2/3	1280 x 720 (25/30 fps)	Y
WDR2/3	720 x 576 (25 fps) 720 x 480 (30 fps)	Y

9.4.1.1.3 *H.264 + H.264 and H.264 + MJPEG*

H.264 + H.264/MJPEG		
TV System	**Stream 1**	**Stream 2**
WDR2	2560 x 1440 (12/15 fps)	1280 x 720 (12/15 fps)
WDR3	2560 x 1440 (12/15 fps)	1280 x 720 (12/15 fps)
		720 x 576 (12 fps) 720 x 480 (15 fps)
WDR2	2560 x 1440 (25/30 fps)	720 x 576 (25 fps) 720 x 480 (30 fps)
WDR2/3	1280 x 720 (25/30 fps)	1280 x 720 (25/30 fps)
		720 x 576 (25 fps) 720 x 480 (30 fps
WDR2/3	720 x 576 (25 fps) 720 x 480 (30 fps)	720 x 576 (25 fps) 720 x 480 (30 fps)

9.4.1.1.4 *H.264 + H.264 + H.264 and H.264 + H.264 + MJPEG*

H.264 + H.264 + H.264			
TV System	**Stream 1**	**Stream 2**	**Stream 3**
WDR2/3	2560 x 1440 (12/15 fps)	1280 x 720 (12/15 fps)	720 x 576 (12 fps) 720 x 480 (15 fps)
		720 x 576 (12 fps) 720 x 480 (15 fps)	
WDR2/3	1280 x 720 (25/30 fps)	1280 x 720 (25/30 fps)	1280 x 720 (25/30 fps)
			720 x 576 (25 fps) 720 x 480 (30 fps
		720 x 576 (25 fps) 720 x 480 (30 fps)	720 x 576 (25 fps) 720 x 480 (30 fps
WDR2/3	720 x 576 (25 fps) 720 x 480 (30 fps)	720 x 576 (25 fps) 720 x 480 (30 fps)	720 x 576 (25 fps) 720 x 480 (30 fps

9.4.1.2 CM-6208 Video Resolution Settings

The following video resolutions are supported:

- H.264-Only
- MJPEG-Only
- H.264 + H.264 and H.264 + MJPEG
- H.264 + H.264 + H.264 and H.264 + H.264 + MJPEG
- H.264 + H.264 + H.264 + H.264 and H.264 + H.264 + H.264 + MJPEG

9.4.1.2.1 *H.264-Only*

H.264-Only				
PAL @ 25 FPS	**NTSC @ 30 FPS**	**PAL @ 50 FPS**	**NTSC @ 60 FPS**	**BNC Support**
3840 x 2160 (24 fps)	3840 x 2160 (24 fps)	-	-	Y
3840 x 2160 (25 fps)	3840 x 2160 (30 fps)	-	-	Y
1920 x 1080 (25 fps)	1920 x 1080 (30 fps)	1920 x 1080 (50 fps)	1920 x 1080 (60 fps)	Y
1280 x 720 (25 fps)	1280 x 720 (30 fps)	1280 x 720 (50 fps)	1280 x 720 (60 fps)	Y
720 x 576 (25 fps)	720 x 480 (30 fps)	720 x 576 (50 fps)	720 x 480 (60 fps)	Y

9.4.1.2.2 *MJPEG-Only*

MJPEG-Only				
PAL @ 25 FPS	**NTSC @ 30 FPS**	**PAL @ 50 FPS**	**NTSC @ 60 FPS**	**BNC Support**
1920 x 1080 (25 fps)	1920 x 1080 (30 fps)	1920 x 1080 (50 fps)	1920 x 1080 (60 fps)	Y
1280 x 720 (25 fps)	1280 x 720 (30 fps)	1280 x 720 (50 fps)	1280 x 720 (60 fps)	Y
720 x 576 (25 fps)	720 x 480 (30 fps)	720 x 768 (50 fps)	720 x 480 (60 fps)	Y

9.4.1.2.3 *H.264 + H.264 and H.264 +MJPEG*

H.264 + H.264/MJPEG (PAL @ 25 FPS)		
Stream 1	**Stream 2**	**BNC Support**
3840 x 2160 (12 fps)	1920 x 1080 (12 fps)	Y on H.264-2 N on MJPEG
3840 x 2160 (20 fps)	1280 x 720 (20 fps)	N
	720 x 576 (20 fps)	Y
1920 x 1080 (25 fps)	1920 x 1080 (25 fps)	N
	1280 x 720 (25 fps)	N
	720 x 576 (25 fps)	Y
1280 x 720 (25 fps)	1280 x 720 (25 fps)	N
	720 x 576 (25 fps)	Y
720 x 576 (25 fps)	720 x 576 (25 fps)	Y

H.264 + H.264/MJPEG (NTSC @ 30 FPS)		
Stream 1	**Stream 2**	**BNC Support**
3840 x 2160 (15 fps)	1920 x 1080 (15 fps)	N
3840 x 2160 (20 fps)	1280 x 720 (20 fps)	N
	720 x 480 (20 fps)	Y
1920 x 1080 (30 fps)	1920 x 1080 (30 fps)	N
	1280 x 720 (30 fps)	N
	720 x 480 (30 fps)	Y
1280 x 720 (30 fps)	1280 x 720 (30 fps)	N
	720 x 480 (30 fps)	Y
720 x 480 (30 fps)	720 x 480 (30 fps)	Y

H.264 + H.264/MJPEG (PAL @ 50 FPS)		
Stream 1	**Stream 2**	**BNC Support**
1920 x 1080 (50 fps)	1280 x 720 (50 fps)	N
	720 x 576 (50 fps)	Y
1280 x 720 (50 fps)	1280 x 720 (50 fps)	N
	720 x 576 (50 fps)	Y
720 x 576 (50 fps)	720 x 576 (50 fps)	Y

H.264 + H.264/MJPEG (NTSC @ 60 FPS)		
Stream 1	**Stream 2**	**BNC Support**
1920 x 1080 (60 fps)	1280 x 720 (60 fps)	N
	720 x 480 (60 fps)	Y
1280 x 720 (60 fps)	1280 x 720 (60 fps)	N
	720 x 480 (60 fps)	Y
720 x 480 (60 fps)	720 x 480 (60 fps)	Y

9.4.1.2.4 *H.264 + H.264 + H.264 and H.264 + H.264 + MJPEG*

H.264 + H.264 + H.264/MJPEG (PAL @ 25 FPS)		
Stream 1	**Stream 2**	**Stream 3**
3840 x 2160 (12 fps)	1920 x 1080 (12 fps)	720 x 576 (12 fps)
1920 x 1080 (25 fps)	1280 x 720 (25 fps)	1280 x 720 (25 fps)
	720 x 576 (25 fps)	720 x 576 (25 fps)
1280 x 720 (25 fps)	1280 x 720 (25 fps)	1280 x 720 (25 fps)
	720 x 576 (25 fps)	720 x 576 (25 fps)
720 x 576 (25 fps)	720 x 576 (25 fps)	720 x 576 (25 fps)

H.264 + H.264 + H.264/MJPEG (NTSC @ 30 FPS)		
Stream 1	**Stream 2**	**Stream 3**
3840 x 2160 (15 fps)	1920 x 1080 (15 fps)	720 x 480 (15 fps)
1920 x 1080 (30 fps)	1280 x 720 (30 fps)	1280 x 720 (30 fps)
	720 x 480 (30 fps)	720 x 480 (30 fps)
1280 x 720 (30 fps)	1280 x 720 (30 fps)	1280 x 720 (30 fps)
	720 x 480 (30 fps)	720 x 480 (30 fps)
720 x 480 (30 fps)	720 x 480 (30 fps)	720 x 480 (30 fps)

H.264 + H.264 + H.264/MJPEG (PAL @ 50 FPS)		
Stream 1	**Stream 2**	**Stream 3**
1920 x 1080 (50 fps)	1280 x 720 (50 fps)	720 x 576 (50 fps)
	720 x 576 (50 fps)	
1280 x 720 (50 fps)	1280 x 720 (50 fps)	720 x 576 (50 fps)
	720 x 576 (50 fps)	
720 x 576 (50 fps)	720 x 576 (50 fps)	720 x 576 (50 fps)

H.264 + H.264 H.264/MJPEG (NTSC @ 60 FPS)		
Stream 1	**Stream 2**	**Stream 3**
1920 x 1080 (60 fps)	1280 x 720 (60 fps)	720 x 480 (60 fps)
	720 x 480 (60 fps)	
1280 x 720 (60 fps)	1280 x 720 (60 fps)	720 x 480 (60 fps)
	720 x 480 (60 fps)	
720 x 480 (60 fps)	720 x 480 (60 fps)	720 x 480 (60 fps)

9.4.1.2.5 *H.264 + H.264 + H.264 + H.264 and H.264 + H.264 + H.264 + MJPEG*

H.264 + H.264 + H.264 + H.264/MJPEG (PAL @ 25 FPS)			
Stream 1	**Stream 2**	**Stream 3**	**Stream 4**
3840 x 2160 (12 fps)	1920 x 1080 (12 fps)	1280 x 720 (12 fps)	720 x 576 (12 fps)
		720 x 576 (12 fps)	
	1280 x 720 (12 fps)	1280 x 720 (12 fps)	
		720 x 576 (12 fps)	
	720 x 576 (12 fps)	720 x 576 (12 fps)	
1920 x 1080 (25 fps)	1920 x 1080 (25 fps)	1280 x 720 (25 fps)	720 x 576 (25 fps)
		720 x 576 (25 fps)	
	1280 x 720 (25 fps)	1280 x 720 (25 fps)	
		720 x 576 (25 fps)	
	720 x 576 (25 fps)	720 x 576 (25 fps)	
1280 x 720 (25 fps)	1280 x 720 (25 fps)	1280 x 720 (25 fps)	720 x 576 (25 fps)
		720 x 576 (25 fps)	
	720 x 576 (25 fps)	720 x 576 (25 fps)	
720 x 576 (25 fps)	720 x 576 (25 fps)	720 x 576 (25 fps)	720 x 576 (25 fps)

H.264 + H.264 + H.264 + H.264/MJPEG (NTSC @ 30 FPS)			
Stream 1	**Stream 2**	**Stream 3**	**Stream 4**
3840 x 2160 (15 fps)	1920 x 1080 (15 fps)	1280 x 720 (15 fps)	720 x 480 (15 fps)
		720 x 480 (15 fps)	
	1280 x 720 (15 fps)	1280 x 720 (15 fps)	
		720 x 480 (15 fps)	
	720 x 480 (15 fps)	720 x 480 (15 fps)	
1920 x 1080 (30 fps)	1920 x 1080 (30 fps)	1280 x 720 (30 fps)	720 x 480 (30 fps)
		720 x 480 (30 fps)	
	1280 x 720 (30 fps)	1280 x 720 (30 fps)	
		720 x 480 (30 fps)	
	720 x 480 (30 fps)	720 x 480 (30 fps)	
1280 x 720 (30 fps)	1280 x 720 (30 fps)	1280 x 720 (30 fps)	720 x 480 (30 fps)
		720 x 480 (30 fps)	
	720 x 480 (30 fps)	720 x 480 (30 fps)	
720 x 480 (30 fps)	720 x 480 (30 fps)	720 x 480 (30 fps)	720 x 480 (30 fps)

H.264 + H.264 + H.264 + H.264/MJPEG (PAL @ 50 FPS)

Stream 1	Stream 2	Stream 3	Stream 4
1920 x 1080 (50 fps)	1280 x 720 (50 fps)	1280 x 720 (25 fps)	720 x 576 (25 fps)
		720 x 576 (50 fps)	720 x 576 (50 fps)
	720 x 576 (50 fps)	720 x 576 (50 fps)	720 x 576 (50 fps)
1280 x 720 (50 fps)	1280 x 720 (50 fps)	1280 x 720 (50 fps)	720 x 576 (50 fps)
	720 x 576 (50 fps)	720 x 576 (50 fps)	
720 x 576 (50 fps)	720 x 576 (50 fps)	720 x 576 (50 fps)	720 x 576 (50 fps)

H.264 + H.264 + H.264 + H.264/MJPEG (NTSC @ 60 FPS)

Stream 1	Stream 2	Stream 3	Stream 4
1920 x 1080 (60 fps)	1280 x 720 (60 fps)	1280 x 720 (30 fps)	720 x 480 (30 fps)
		720 x 480 (60 fps)	720 x 480 (60 fps)
	720 x 480 (60 fps)	720 x 480 (60 fps)	720 x 480 (60 fps)
1280 x 720 (60 fps)	1280 x 720 (60 fps)	1280 x 720 (60 fps)	720 x 480 (60 fps)
		720 x 480 (60 fps)	
	720 x 480 (60 fps)	720 x 480 (60 fps)	
720 x 480 (60 fps)	720 x 480 (60 fps)	720 x 480 (60 fps)	720 x 480 (60 fps)

9.4.1.3 Text Overlay Settings

Select the relevant checkbox for the data to include in the on-screen display:

- *Include date*
- *Include time*
- *Include text string* – when this checkbox is selected, enter the string in the text box that opens.
- *Include subtitle* – when this checkbox is selected, enter the string in the text box that opens.

9.4.1.4 Video Rotate Type

You can change video display type if necessary. Selectable video rotate types include *Normal video, Flip video, Mirror video,* and *180 degree rotate*. Differences among these types are illustrated below. Suppose the displayed image of the camera is shown as follows.

Figure 94: View-1 (Source)

To rotate the image vertically, for example, select *Flip video*. The displayed image is reversed as shown below.

Figure 95: View-2 Image Rotated Vertically (Reversed)

Following are descriptions of different video rotate types.

- *Normal video* – The image appears as it is viewed. This is the default setting.
- *Flip video* – The image is reversed along its horizontal axis.
- *Mirror video* – The image is reversed along its vertical axis.
- *180 degree rotate* – The image rotates 180° counter-clockwise (to the left).

Click **SAVE** to confirm the setting.

9.4.1.5 GOV Settings

Users can set the GOV length to determine the frame structure (I-frames and P-frames) in a video stream for saving bandwidth. The setting range is from 2 to 64. A longer GOV means decreasing the frequency of I-frames. The default GOV setting for H.264-1 and H.264-2 is 50 {PAL)/60 (NTSC). The default GOV setting for H.264-3 and H.264 (CM-6208 only) is 25 (PAL)/30 (NTSC). Click **SAVE** to confirm the GOV setting.

9.4.1.6 H.264 Profile

The H.264 standard defines 21 sets of capabilities. These are referred to as profiles and they target specific classes of applications. In the security industry, the most common are as follows:

- **Baseline Profile (BP)**
  Primarily for low-cost applications that require additional data loss robustness, such as videoconferencing and mobile applications. This is the most common profile used in IP security cameras due to the low computational cost of processing the video.
- **Main Profile (MP)**
  This profile provides improved picture quality at reduced bandwidths and storage costs and is becoming more common as the camera processors (DSPs) become more able to handle the processing load. *Main Profile* can save 10-12% over *Baseline*. This is the default profile.
- **High Profile (HP)**
  High Profile is the primary profile for HD broadcast applications. It can save 10-12% of the storage cost over *Main Profile*. However, it may also increase video latency, depending on the stream structure. Quasar Gen II models default to the *Main Profile* to provide the best trade-off between storage size and video latency.

Click **SAVE** to confirm the settings.

9.4.2 Video Compression

From the **Video Compression** page, you can specify MJPEG and H.264 compression settings.

CM-6204 cameras support three video streams.

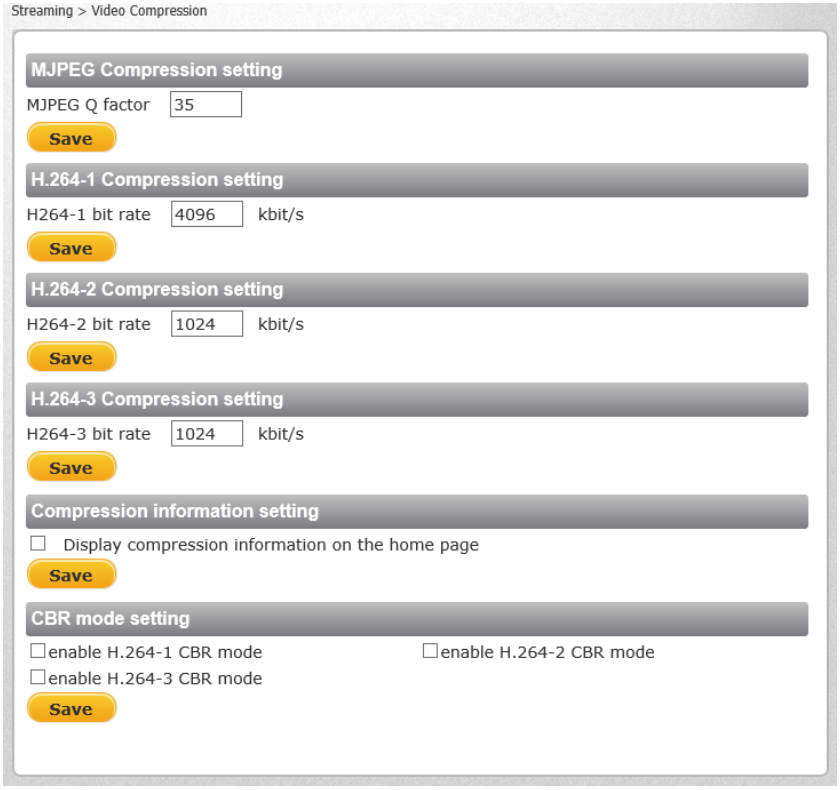


Figure 96: CM-6204 Video Compression Screen

CM-6208 cameras support four video streams.

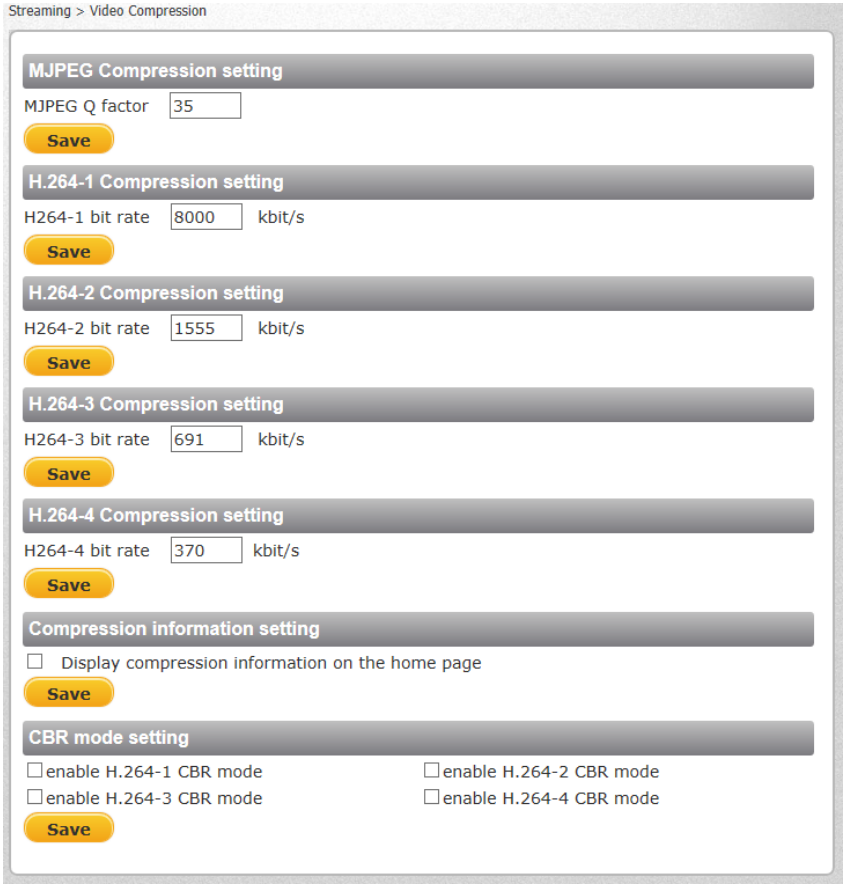


Figure 97: Video Compression Screen

MJPEG Compression Setting

A higher value implies higher bit rates and higher visual quality. The default setting of the MJPEG Q factor is 35. The setting range is from 1 to 70. Click **SAVE** to confirm the setting.

H.264 Compression Setting

The default setting of H.264-1 is 4096. The default setting for the other streams is 1024 kbps. The setting range is from 64 to 20,480 kbps. Click **SAVE** to confirm the setting.

Note:
A total of 26,624 kbps is available on the camera for streaming. A single stream is limited to 20,480 kbps

CBR Mode Setting

If available bandwidth is limited, select CBR (Constant Bit Rate) mode. To operate the camera in Variable Bit Rate (VBR) mode, uncheck the CBR checkbox. Click **SAVE** to confirm the setting.

Note:
CBR mode affects image quality.

9.4.3 Video ROI Encoding

It is possible to configure Region of Interest settings for three (CM-6204) or four (CM-6208) H.264 streams on the **Video ROI Encoding** screen. The image displayed within the ROI box can be displayed with a higher bit rate and quality than the image outside of the box. Overall bit rate is not affected by selecting Regions of Interest. Enhancing the video where the quality is very important consumes more bandwidth, but enables lowering image quality and bandwidth consumption on less important zones in the scene.

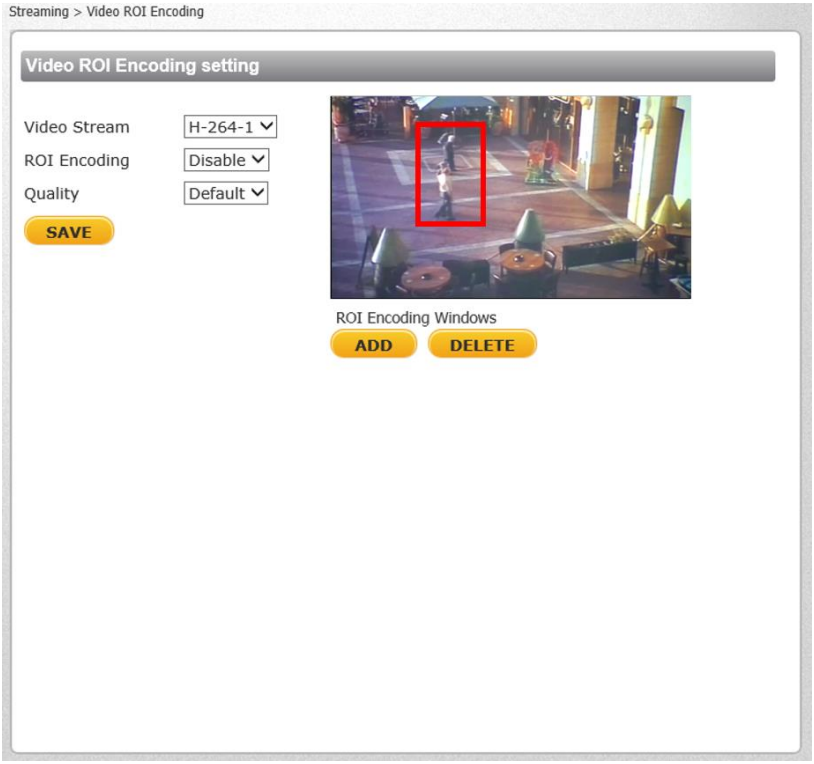


Figure 98: Video ROI Encoding Screen

To use ROI encoding

1. From the *Video Stream* drop-down menu, select the H.264 stream.
2. From the *ROI Encoding* drop-down menu, select *Enable* to activate this function.
3. From the *Quality* drop-down menu, select a number between -15 (lowest image quality) to +15 (highest image quality) or default (where the image quality of the video in the box is the same as the image quality outside the box).
4. Click **SAVE** when finished.
5. Drag the box in the ROI Encoding Window to cover the zone for which you want to activate ROI encoding.
6. Click **ADD** to create a new zone or **DELETE** to remove a zone.
7. Click **SAVE** when finished.

9.4.4 Video OCX Protocol

From the **Video OCX Protocol** page, you can select various protocols for streaming media over the network. In the case of multicast networking, select *Multicast mode*. Three streams are available on CM-6204 cameras. Four streams are available on CM-6208 cameras.

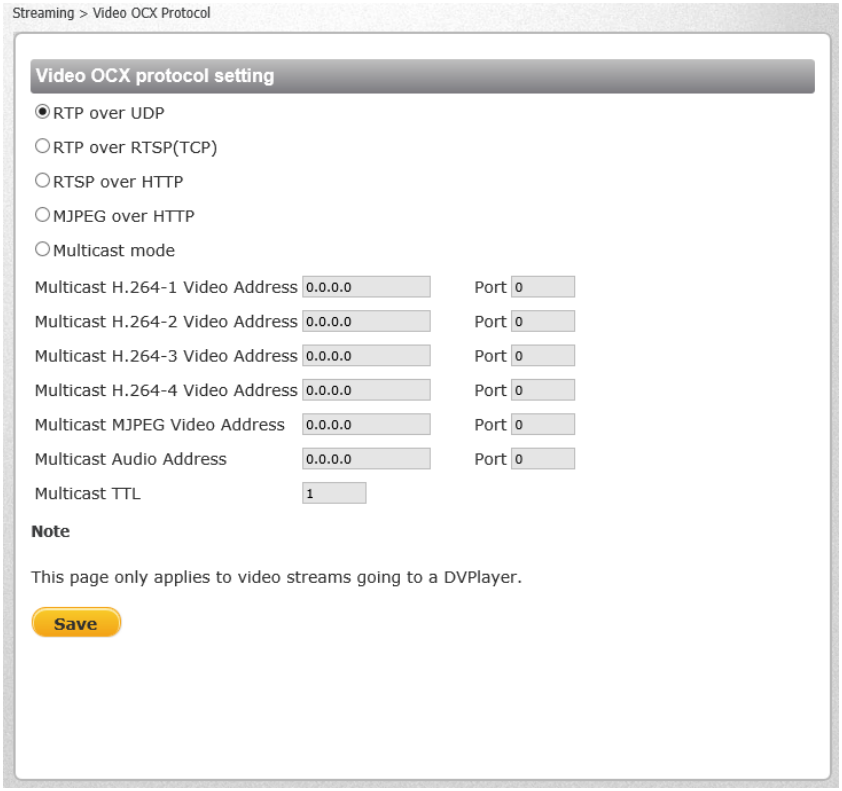

Streaming > Video OCX Protocol
Video OCX protocol setting
RTP over UDP
RTP over RTSP(TCP)
RTSP over HTTP
MJPEG over HTTP
Multicast mode
Multicast H.264-1 Video Address 0.0.0.0 Port 0
Multicast H.264-2 Video Address 0.0.0.0 Port 0
Multicast H.264-3 Video Address 0.0.0.0 Port 0
Multicast H.264-4 Video Address 0.0.0.0 Port 0
Multicast MJPEG Video Address 0.0.0.0 Port 0
Multicast Audio Address 0.0.0.0 Port 0
Multicast TTL 1
Note
This page only applies to video streams going to a DVPlayer.
Save

Figure 99: Video OCX Protocol Screen

Video OCX protocol setting options include:

- *RTP over UDP*
- *RTP over RTSP (TCP)*
- *RTSP over HTTP*
- *MJPEG over HTTP*
- *Multicast mode* – Enter in each field all required data, including *Multicast H.264-1 Video Address, Multicast H.264-2 Video Address, Multicast H.264-3 Video Address, Multicast H.264-4 Video Address (CM-6208 only), Multicast MJPEG Video Address, Multicast Audio Address,* and *Multicast TTL*.

Click **SAVE** to confirm the settings.

9.4.5 Video Frame Rate

From the **Video Frame Rate** screen, you can specify the frames per second (fps) for each video compression format. CM-6204 includes three streams. CM-6208 includes four streams.

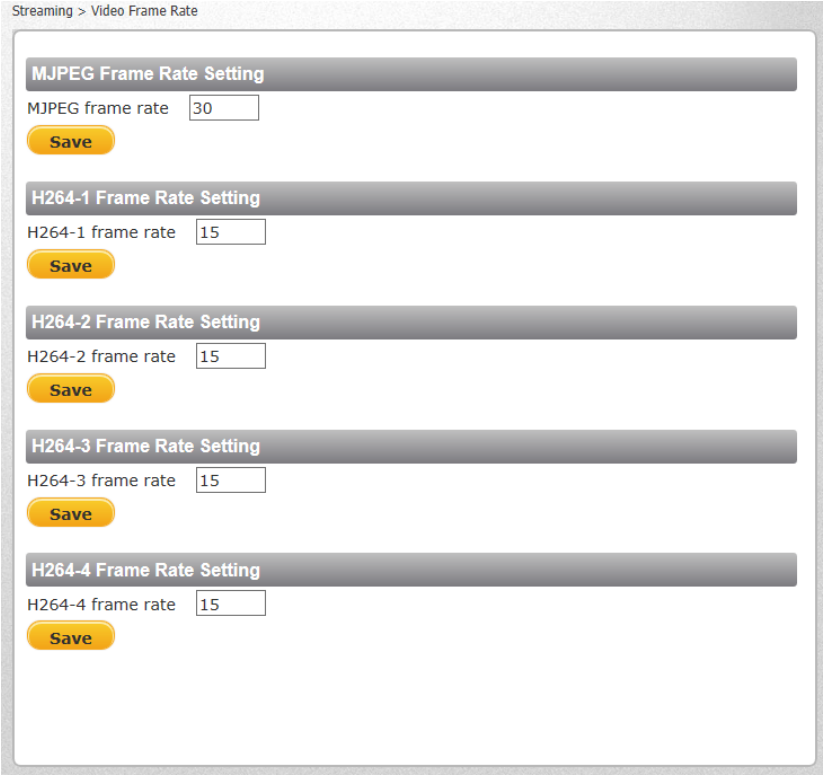


Figure 100: Video Frame Rate Screen

MJPEG/H.264 Frame Rate Setting

When operating the unit in H.264-only mode, the default frame is 30 fps in NTSC and 25 fps in PAL.

Note:
A lower frame rate decreases video smoothness.

The following settings apply when operating the unit in any mode other than H.264–only:

- *MJPEG* – The setting range of the MJPEG Frame Rate is from 1 to 60 in NTSC and 1 to 50 in PAL. The default setting is 30 fps in NTSC and 25 fps in PAL.
- *H.264-1* – The setting range for the H-264-1 Frame Rate is from 1 to 15 in NTSC and 1 to 12 in PAL. The default setting is 15 fps in NTSC and 12 fps in PAL.
- *H.264-2* – The setting range for the H-264-2 Frame Rate is from 1 to 15 in NTSC and 1 to 12 in PAL. The default setting is 15 fps in NTSC and 12 fps in PAL.
- *H.264-3* – The setting range for the H-264-3 Frame Rate is from 1 to 30 in NTSC and 1 to 50 in PAL. The default setting is 15 fps in NTSC and 12 fps in PAL.
- *H.264-4 (CM-6208 only)*– The setting range for the H-264-4 Frame Rate is from 1 to 30 in NTSC and 1 to 50 in PAL. The default setting is 15 fps in NTSC and 12 fps in PAL.

Note:
Images can be sent by FTP or e-mail only when MJPEG is selected from the Streaming > Video Resolution screen.

Click **SAVE** to confirm the settings.

9.4.6 Video Mask

From the **Mask** screen, you may select up to five rectangular portions of the View Area to 'Mask.' Below is an illustration with the maximum five masks displayed in the View Area, the last (fifth) one selected being highlighted in red.

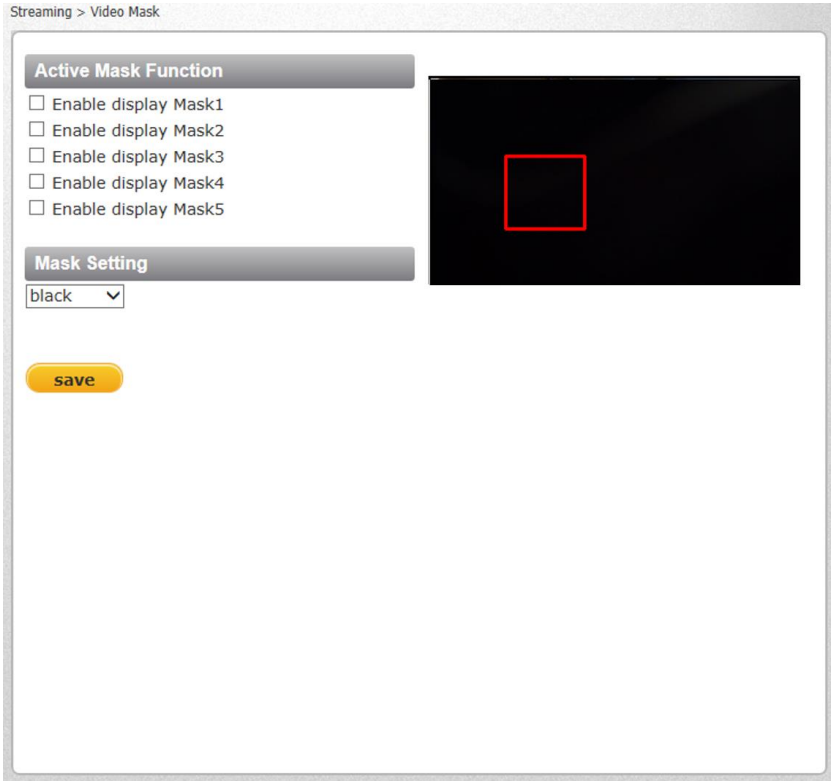


Figure 101: Mask Screen

Active Mask Function

When a Video [Privacy] Mask is turned on, the area within the mask or box is blocked out or obscured from view.

To enable a mask

1. Check a *Video Mask* checkbox. A red frame is displayed in the Live Video pane on the right side.
2. Use the mouse to drag and drop, adjust the mask's size, and place it on the target zone.

> **Note:**
> It is suggested to set the Video Mask twice as large as the object it covers.

To disable a mask

1. Uncheck the checkbox of the Video Mask meant to be deleted. The selected mask disappears from the Live Video pane.

Mask Setting

- Mask color – The selections of Mask color include red, black, white, yellow, green, blue, cyan, and magenta.

Click **Save** to confirm the setting.

9.4.7 Audio

From the **Audio** screen you can select the Transmission Mode, Server Gain, Bit Rate, and enable or disable storage of the audio recording.

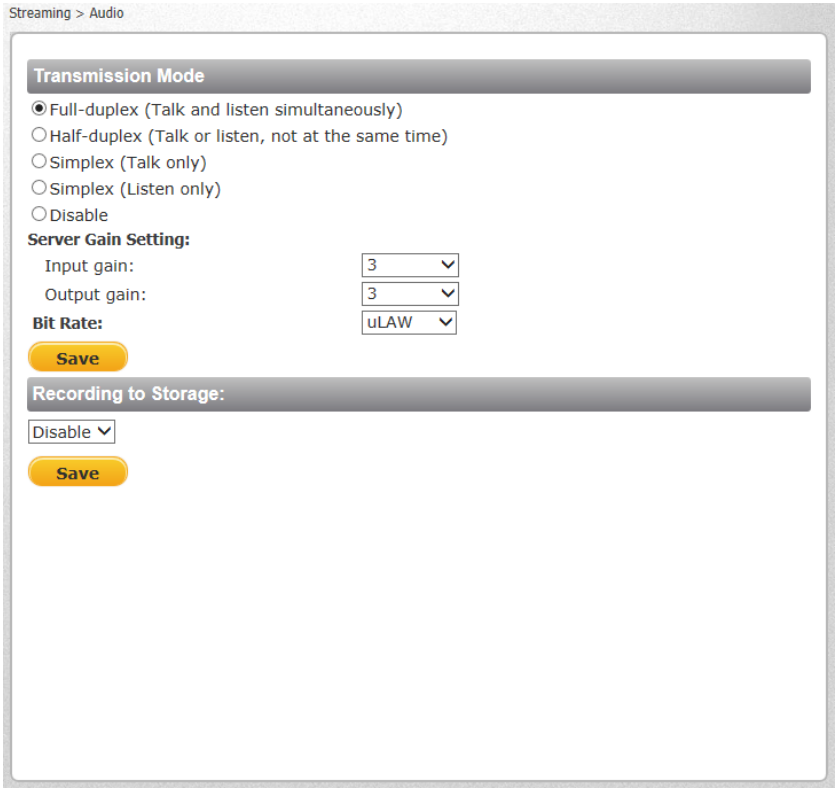


Figure 102: Audio Screen

Transmission Mode

- *Full-duplex (Talk and listen simultaneously)* – In the Full-duplex mode, the local and remote sites can communicate with each other simultaneously, i.e. both sites can speak and be heard at the same time.
- *Half-duplex (Talk or listen, not at the same time)* – In the Half-duplex mode, the local or remote site can only talk or listen to the other site at one time.
- *Simplex (Talk only)* – In the Talk only Simplex mode, the local/remote site can only talk to the other site.
- *Simplex (Listen only)* – In the Listen only Simplex mode, the local/remote site can only listen to the other site.
- *Disable* – Select this option to turn off the audio transmission function.

Server Gain Setting

Set the audio input/output gain levels for sound amplification. The audio gain values are adjustable from 1 to 6. The sound will be turned off if the audio gain is set to *Mute*.

Bit Rate

Selectable audio transmission bit rate include 16 kbps (G.726), 24 kbps (G.726), 32 kbps (G.726), 40 kbps (G.726), µLAW (G.711) and ALAW (G.711). Both µLAW and ALAW signify 64 kbps, but in different compression formats. A higher bit rate enables higher audio quality, but requires higher bandwidth.

Note:
Latitude does not support G.726.

Click **SAVE** to confirm the settings.

Recording to Storage

This function enables recording of the audio on the SD card and NAS. The *Recording to Storage* function may be enabled or disabled in the **Audio** screen. The default setting is *Disabled.*

Note:
This function works only if the *Recording to Storage* option has been selected or if the *Schedule* option has been set.

Click **SAVE** to confirm the settings.

9.5 Camera Settings

From the **Camera** tab, the administrator can adjust any of the camera settings from the following tabs:

- Exposure
- Picture Adjustment
- Advanced Picture Settings
- IR Function
- Miscellaneous

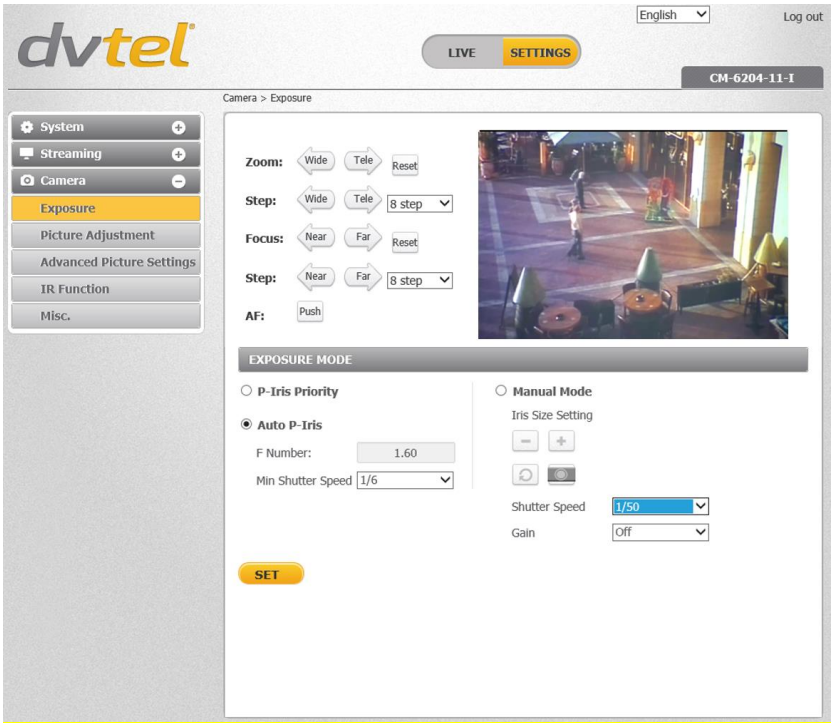


Figure 103: Camera Section Tabs

Every screen in the **Camera** section includes the following pushbuttons to the left of the Live View window:

Zoom				Click the **Wide** or **Tele Zoom** button to implement continuous zoom adjustment. Click **Reset** to return the zoom to the default setting.
Step				Click the **Wide** or **Tele Step** button to alternate the zoom between wide and telephoto views within a user-defined range of steps, which can be selected from the drop-down menu.
Focus				Click the **Near** or **Far Focus** button to implement continuous focus adjustment. Click **Reset** to return the zoom to the default setting.
Step				Click the **Near** or **Far Step** button to alternate the focus between near and far views within a user-defined range, which can be selected from the drop-down menu.
AF				Click the **Push AF** button once to adjust zoom or focus.

9.5.1 Exposure

The **Exposure** screen is used to configure lens settings and exposure modes. The exposure is the amount of light received by the image sensor and is determined by the amount of exposure by the sensor (shutter speed), and other exposure parameters.

Administrators may either allow the camera to automatically select an exposure level using a programmed algorithm or choose the level themselves. Even in *Auto Mode*, a Minimum Shutter Speed may be set from the drop-down menu to ensure a maximum level of exposure. In *Manual Mode*, the administrator can choose fixed shutter speeds from a drop-down menu. The smaller the number (the higher the shutter speed) that the administrator selects, the lower the exposure level and vice versa.

The bottom section of the screen enables you to select one of three exposure modes: P-Iris Priority, Auto P-Iris (default), or Manual Mode. Administrators may either allow the camera to automatically select an exposure level using a programmed algorithm or choose the level themselves

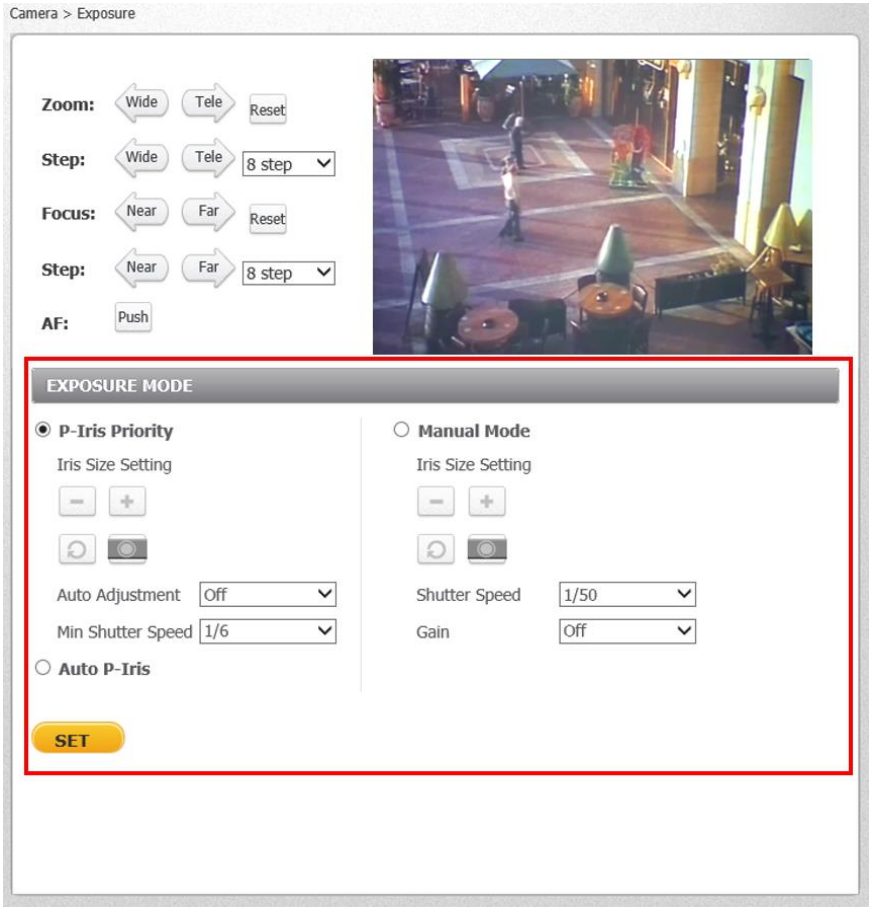


Figure 104: CM-6204 Exposure Screen

P-Iris Priority Mode

In P-iris Priority mode, the iris does not adjust, regardless of the light level. If, however, the light level goes below the P-iris setting, the iris will fully open in a single step if the *Auto Adjustment* option is turned on.

The following setting are available:

- *Iris Size Setting* – Select the following buttons:

	The minus (-) button closes the iris.
	The plus (+) button opens the iris.
	The reset button is for resetting the P-iris
	The radial button is for automatically selecting the optimal iris exposure.

- *Auto Adjustment* – From the drop-down menu, select *On* or *Off*. When enabled, if the lighting level falls below the set P-iris level, the iris will jump to its fully-opened position.
- *Min Shutter Speed* – When selecting this mode, the camera's shutter speed automatically achieves a consistent video output level. Users can select a suitable shutter speed according to the environmental luminance.
  - On CM-6204, the shutter speed range is selectable on the drop-down menu from 1/2 to 1/500 sec (NTSC) and 1/3 to 1/425 sec (PAL).
  - On CM-6208, the shutter speed range is selectable on the drop-down menu from 1 to 1/500 sec (NTSC) and 1/3 to 1/425 sec (PAL).

P-Iris Priority – Min Shutter Speed	
PAL	**NTSC**
1/425	1/500
1/300	1/350
1/215	1/250
1/150	1/180
1/120	1/120
1/100	1/100
1/75	1/90
1/50	1/60
1/25	1/30
1/12	1/15
1/6	1/8
1/3	1/4
1/1.5 (CM-6208)	½
	1 (CM-6208)

Click **SET** when you finish configuring the settings.

Auto P-Iris Mode

Auto-P iris is the default mode. It automatically and smoothly adjusts the iris when the light level drops to a point where it is insufficient to support the P-iris setting. A Minimum Shutter Speed may be set from the drop-down menu to ensure a maximum level of exposure.

The following setting are available:

- *Min Shutter Speed* – When selecting this mode, the shutter is completely open and the exposure priority is given to the iris. Shutter speed and AGC circuit function automatically in cooperating with the iris to achieve a consistent exposure output.
  - On CM-6204, the shutter speed range is from 1/2 to 1/30 sec (NTSC) and 1/3 to 1/25 sec (PAL).
  - On CM-6208, the shutter speed range is from 1 to 1/30 sec (NTSC) and 1/1.5 to 1/25 sec (PAL).

Auto Iris - Min Shutter Speed	
PAL	**NTSC**
1/25	1/30
1/12	1/15
1/6	1/8
1/3	1/4
1/1.5 (CM-6208)	½
	1 (CM-6208)

- *F Number* – Displays the current F-Stop setting.

Click **SET** when you finish configuring the settings.

Manual Mode

Manual Mode opens the iris completely with a fixed gain to a fixed shutter speed. Users can select a suitable shutter speed according to the environmental luminance.

In Manual Mode, the administrator can select a fixed shutter speed and gain from drop-down menus. The smaller the shutter speed number (the higher the shutter speed), the lower the exposure level. The higher the gain, the brighter the picture.

Manual mode is used generally where light levels are fixed and the auto settings do not provide the perfect exposure. It is recommended for scenes where there is a fixed lighting contrast and a constant, precise exposure is required.

The following setting are available:

- *Iris Size Setting* – Select the following buttons

	The minus (-) button closes the iris.
	The Plus (+) button opens the iris.
	The reset button is for resetting the P-iris
	The radial button is for automatically selecting the optimal iris exposure

- *Shutter Speed* – Users should select the suitable shutter speed according to the environmental luminance.
  - On CM-6204, the fixed shutter speed is selectable from 1/2 to 1/10000 sec (NTSC) and 1/3 to 1/10000 sec (PAL).
  - On CM-6208, the fixed shutter speed is selectable from 1 to 1/10000 sec (NTSC) and 1/1.5 to 1/10000 sec (PAL).

Manual Mode - Fixed Shutter Speeds	
PAL	**NTSC**
1/10000	1/10000
1/3500	1/3000
1/2500	1/2000
1/1250	1/1000
1/600	1/725
1/425	1/500
1/300	1/350
1/215	1/250
1/150	1/180
1/120	1/120
1/100	1/100
1/75	1/90
1/50	1/60
1/25	1/30
1/12	1/15
1/6	1/8
1/3	1/4
1/1.5 (CM-6208)	½
	1 (CM-6208)

- *Gain* – A nominal video signal level is usually 1 volt peak-to-peak for composite video, 0.7 volts for component or RGB video, or 0.3 volts for the chrominance subsection, at which level a fully saturated picture is transmitted to the acceptor. However, for cases where the video signal is attenuated, a low-noise, high-gain analog amplifier is built into quality video processing equipment. This amplifier provides video gain control whereby the video signal can be boosted or reduced. Dark pictures caused by low level lighting are easily adjusted. The *Gain* drop-down menu turns the video gain *Off* or moves it in steps from 1 to 9.

Click **SET** when you finish setting the gain.

9.5.2 Picture Adjustment

Adjustment of some qualities of the video is made possible by selecting *Picture Adjustment* in the **Camera** tab. Brightness, Sharpness, Contrast, Saturation and Hue may all be adjusted via drop-down menus from this window, as shown below.

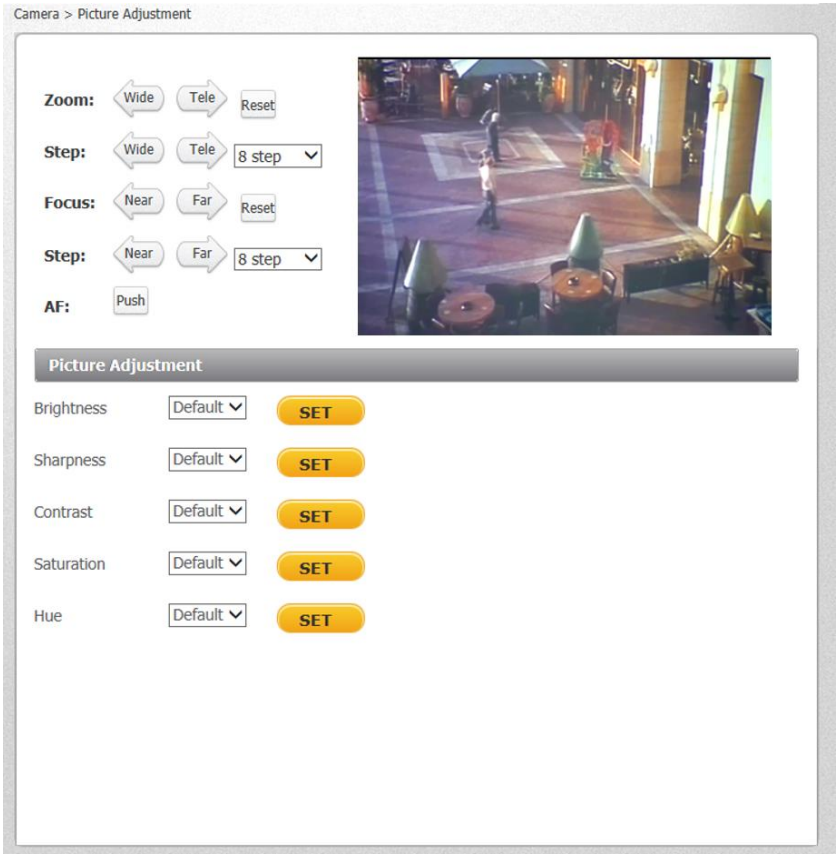


Figure 105: Camera Settings Screen – Picture Adjustment

9.5.2.1 Brightness

You can adjust the image's brightness by adjusting this parameter. Select from the range between -12 to +13. To increase video brightness, select a larger number. Click **SET** to confirm the new setting.

9.5.2.2 Sharpness

Increasing the sharpness level can make the image look sharper, especially enhancing the object's edge. Select from the range between 0 to +15. Click **SET** to confirm the new setting.

9.5.2.3 Contrast

Camera image contrast level is adjustable. Select from a range of -6 to +19. Click **SET** to confirm the new setting.

9.5.2.4 Saturation

Camera image saturation level is adjustable. Select from a range of -6 to +19. Click **SET** to confirm the new setting.

9.5.2.5 Hue

Camera image hue level is adjustable: select from a range of -12 to +13. Click **SET** to confirm the new setting.

9.5.3 Advanced Picture Settings

9.5.3.1 White Balance

Options for controlling the camera's white balance (color balance) are shown below.

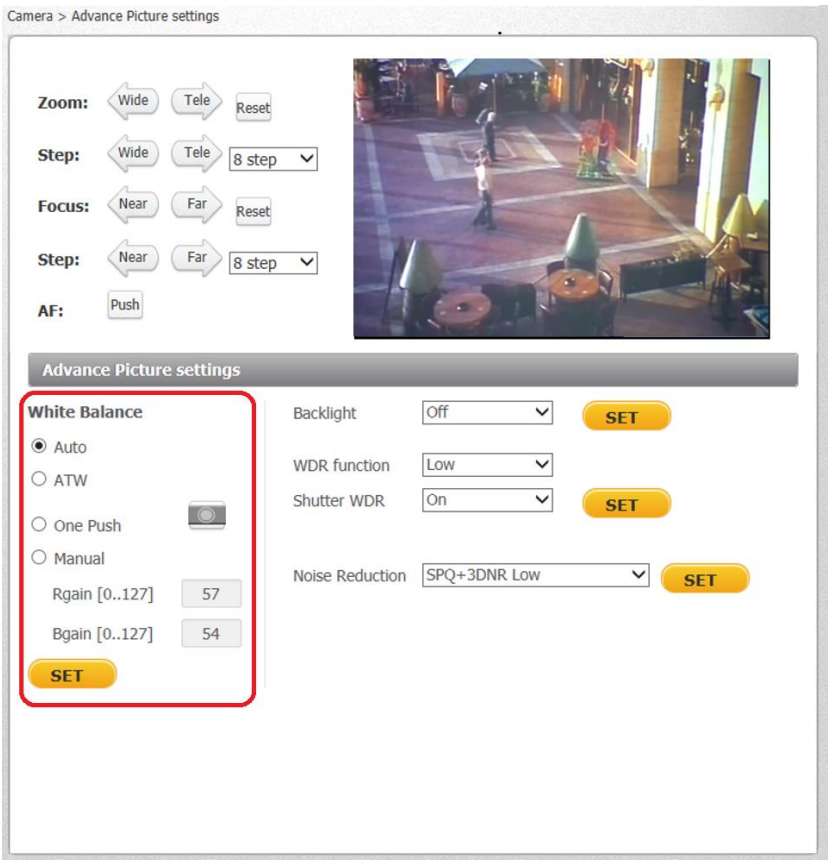


Figure 106: Advanced Picture Settings Screen – White Balance

A camera needs to find a reference color temperature as a way of measuring the quality of a light source for calculating all other colors. The unit for measuring this ratio is in Kelvin (°K) degrees. You can select one of the White Balance control modes according to the operating environment. The table below shows the color temperature of some light sources for reference.

Light Sources	Color Temperature in K
Cloudy Sky	6,000 to 8,000
Noon Sun and Clear Sky	6,500
Household Lighting	2,500 to 3,000
75-watt Bulb	2,820
Candle Flame	1,200 to 1,500

Four white balance modes are available:

- *Auto* – The Auto Balance White mode computes the white balance value output using color information from the entire screen. It is suitable for an environment with a light source color temperature in the range of approximately 2,700 ~ 7,500K.
- *ATW (Auto Tracking White Balance)* – The Auto Tracking White Balance function automatically adjusts the white balance in a scene while temperature color is changing. The ATW Mode is suitable for an environment with a light source color temperature in the range of approximately 2500 ~ 10,000K.
- *One Push* – This button activates the factory-optimized setting for white balance. This setting may not be ideal for every lighting environment.
- *Manual* – In this mode, you can manually change the white balance value. You can select a number between 0 – 127 for either/both Rgain and Bgain to increase the red and/or blue luminance.

Click **SET** to confirm the new settings.

9.5.3.2 Backlight

The Backlight Compensation function prevents the center object from being too dark in surroundings where excessive light is behind the center object. Select *On* or *Off*.

Click **SET** to confirm the new settings.

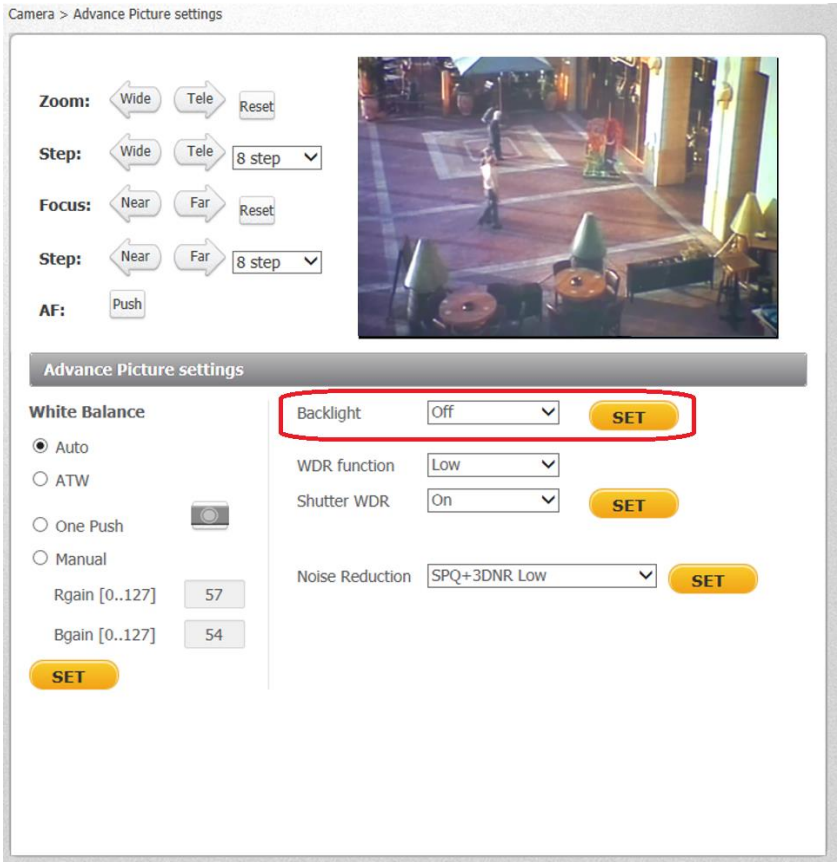


Figure 107: Advanced Picture Settings Screen – Backlight

9.5.3.3 WDR Function and Shutter WDR

The WDR (Wide Dynamic Range) function resolves high contrast or changing light issues in order to enhance the video display.

The *WDR function* setting is adjustable among *Off*, *Low, Mid* and *Hi*. A higher level of WDR represents wider dynamic range, so that the IP camera can capture a greater scale of brightness.

The Shutter WDR function is a form of multi-exposure WDR, which is implemented by using a combination of slow- and fast-exposure shutters. The camera uses an algorithm to determine the optimal mix of light and dark regions within the scene from the two shutters in order to adjust the wide dynamic range of the scene. The *Shutter WDR* setting is selectable between *On* or *Off:*

- When *On* is selected, the image has a wide dynamic range, so that the IP camera can capture a greater scale of brightness.
- Selecting *Off* disables this function. This is the default setting.

Click **SET** to confirm the new settings.

Note:
Shutter WDR is available only on the CM-6204 model.

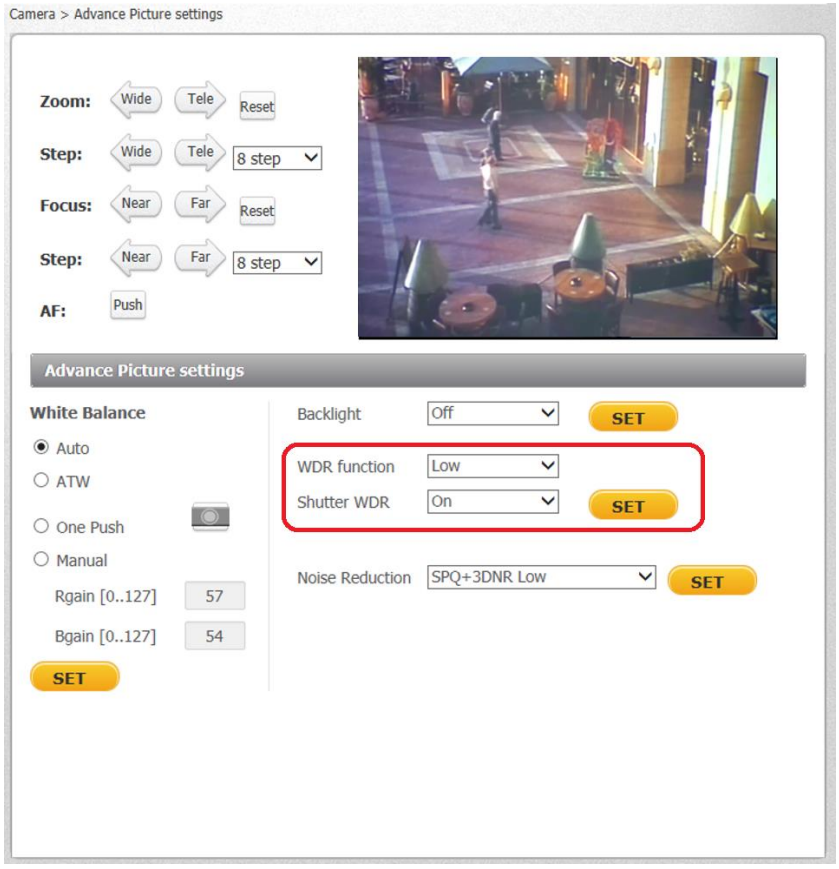


Figure 108: Advanced Picture Settings Screen – WDR Function

9.5.3.4 Noise Reduction

Different level options for 3D Noise Reduction (3DNR) include *Low, Mid* and *High*. A higher level of 3DNR generates relatively enhanced noise reduction.

The proprietary Smart Picture Quality (SPQ) video processing method can drastically minimize motion blur and provides clear images even in low-light environment. The combination of SPQ and 3DNR at different levels further yields exceptional video performance in various conditions.

The Noise Reduction function reduces image noise/snow, enabling the IP camera to deliver clearer images in low-light conditions. The Noise Reduction is adjustable from *Off, 3DNR Low, 3DNR Mid, 3DNR Hi, SPQ, SPQ + 3DNR Low, SPQ + 3DNR Mid,* to *SPQ + 3DNR Hi.*

Click **SET** to confirm the new settings.

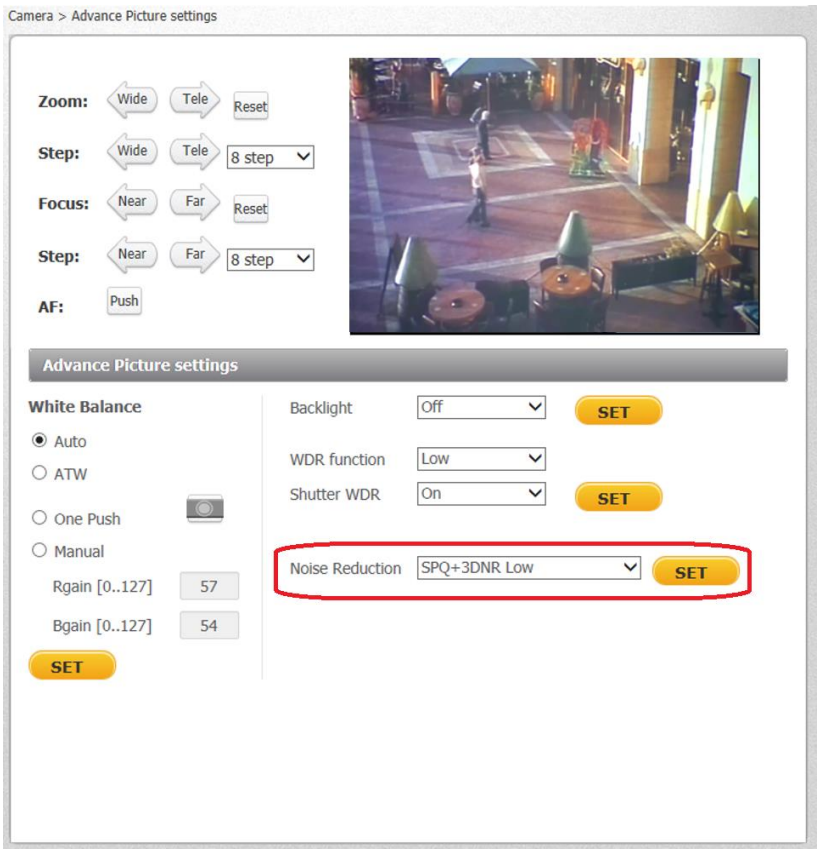


Figure 109: Advanced Picture Settings Screen – Noise Reduction

9.5.4 IR Function

The IR Function setting activates two functions. It activates the IR LED illuminator for use in low-light conditions or at night and activates *IR mode*, which is the IR Cut (IRC) filter for electronic day/night operation.

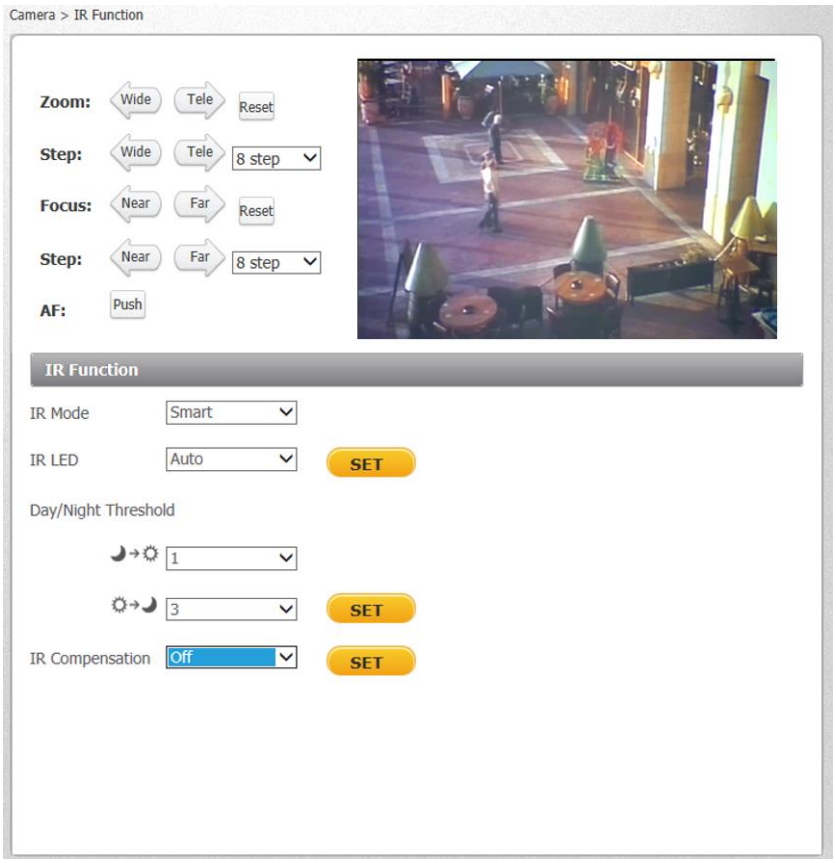


Figure 110: IR Function Screen

9.5.4.1 IR Mode

The day/night IRC switching mechanism operates according to the ambient light level rather than activation of the IR LED mode. The *IR Mode* drop-down menu enables you to select from *Auto/On/Off/Smart* modes. The default mode is *Smart*. Following is an explanation of the four settings:

- *Auto Mode* – The camera converts from Day mode (color) to Night mode (monochrome) automatically at nighttime or in low light conditions. When there is sufficient light, the camera converts automatically from Night mode to Day mode.
- *On* – Activates IR mode (puts camera into monochrome/Night mode).
- *Off* – Deactivates IR mode (puts camera into color/Day mode).
- *Smart* – Smart mode enhances monochrome/Night mode stability when IR illumination is dominant and keeps the camera from switching between Day and Night modes. In this mode, the IR Cut filter is on (i.e. monochrome/Night mode) when the IR LED illuminator also is activated. This prevents the camera from returning to color/Day mode.

Click **SET** to confirm the new setting.

9.5.4.2 IR LED Illuminator

This setting is used in low-light conditions or at night. IR LED lights are turned *On* or *Off*, depending on the light sensor. The default mode is *Auto.* Two settings are available:

- *Auto* – The light sensor operates automatically.
- *Off* – The IR light is always off.

Click **SET** to confirm the new setting.

9.5.4.3 Day/Night Threshold

Set the threshold at which you want to activate the IR function:

- For the daytime to nighttime threshold, from the upper drop-down list, select a number between 1-9, where 1 is darker and 9 is brighter.
- For the nighttime to daytime threshold, from the upper drop-down list, select a number between 1-9, where 1 is darker and 9 is brighter.

Click **SET** to confirm the new setting.

9.5.4.4 IR Compensation

From the drop-down list, set the IR Compensation to *On* or *Off*. Setting IR Compensation to *On* compensates for the reflection of infrared light emitted from the camera onto reflective objects, thus improving image sharpness and definition. Without IR compensation, objects may appear blurred.

Click **SET** to confirm the new setting.

9.5.5 Miscellaneous

From the **Misc.** (Miscellaneous) tab, you can set the Digital Zoom and TV System.

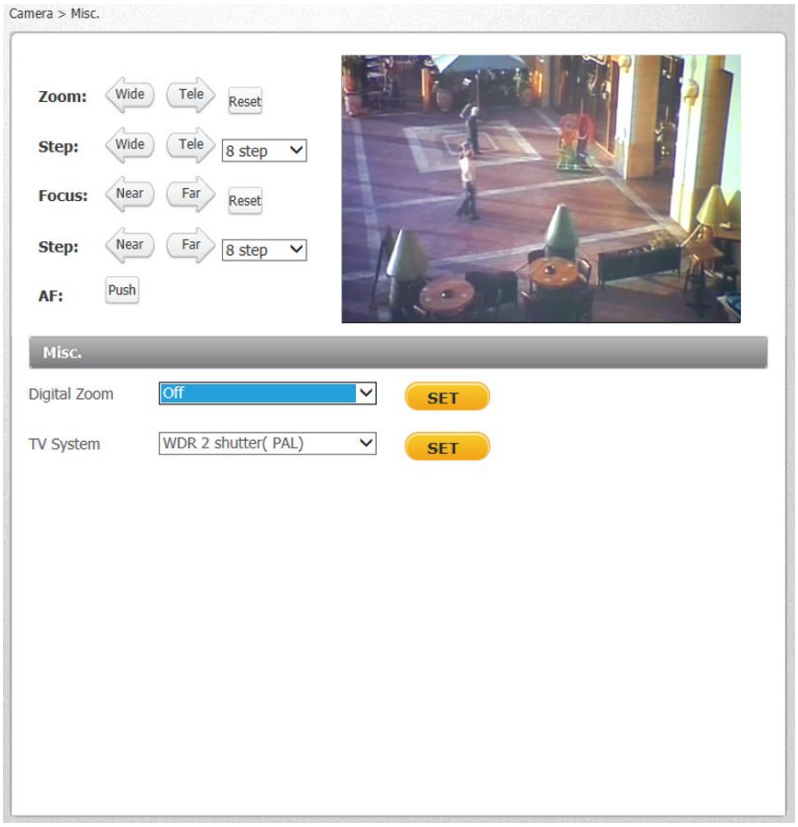


Figure 111: Camera Settings Screen – Digital Zoom

9.5.5.1 Digital Zoom

The camera's digital zoom is adjustable from x2 to x10. Select the desired zoom or *Off*.

Click **SET** to confirm the new setting.

9.5.5.2 TV System

The *TV System* options depend on the model.

Note:
After changing the video format, the camera restarts automatically. You must re-enter the unit's IP address again in your browser in order to use the unit with the new settings.

9.5.5.2.1 *CM-6204 TV System Settings*

Select one of two WDR settings according to your TV standard: *WDR 2 shutter (NTSC), WDR 2 shutter (PAL), WDR 3 shutter (NTSC), or WDR 3 shutter (PAL).*

The WDR2 shutter setting is composed of one short exposure and one long exposure taken simultaneously and then composited to create the image. The WDR2 shutter setting is recommended for most situations.

The WDR3 shutter setting is composed of three exposures – short, medium, and long – taken simultaneously and then composited to create the image. The WDR3 shutter setting is recommended for more complicated scenes with difficult lighting.

Click **SET** to confirm the setting.

9.5.5.2.2 *CM-6208 TV System Settings*

Select the video system and WDR setting according to the desired frame rate and the TV standard: *25 fps (PAL), 30 fps (NTSC), 50 fps (PAL),* or *60 fps (NTSC).*

9.6 Log Out

Selecting the **Logout** link on the Home page to close the session. The following message appears:

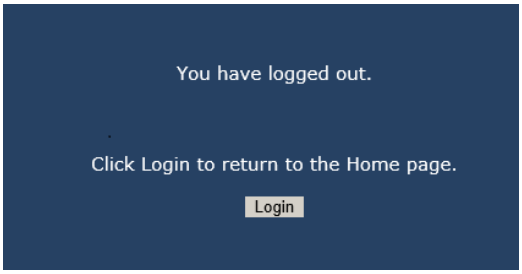


Figure 112: Login Message

Upon clicking **Login,** the **Login** window opens.

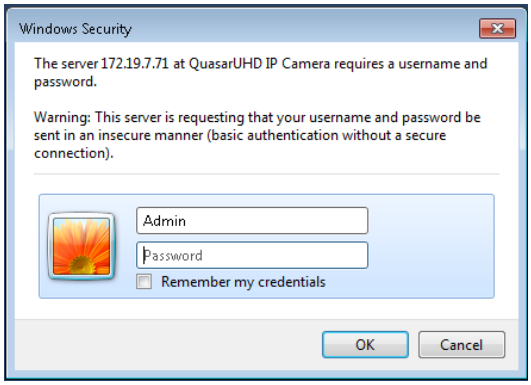

Windows Security
The server 172.19.7.71 at QuasarUHD IP Camera requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
Admin
Password
Remember my credentials
OK
Cancel

Figure 113: Login Window

10 Appendices

- CM-6204 Technical Specifications
- CM-6208 Technical Specifications
- Device Search Software
- Internet Security Settings
- Install UPnP Components
- Deleting Existing DVPlayer
- Deleting Temporary Internet Files
- Connecting Leads to a Spring Clamp Terminal Block
- Mounting Accessories

A.1. CM-6204 Technical Specifications

Camera			
Image Sensor		1/3” 2688 x 1520 Progressive Scan BSI CMOS	
Effective Pixels		2560 x 1440 (H x V)	
Shutter Speed		1.0 to 1/10,000 (auto)	
Digital Slow Shutter (DSS)		1/1 to 1/25 or 1/30 with <32x sensitivity boost in day/night mode	
Sensitivity		0.3 Lux @F1.4 in day (color) mode; 0.04 Lux @ F1.4 in night (B/W) mode with IR illuminator ON, measured with DSS OFF at 30 IRE	
Enclosure		Tamper-resistant surface mount plastic case	
Lens		**CM-6204-11-I**	**CM-6204-21-I**
Lens Type		Varifocal Motorized P-Iris with auto focus and True Day/Night	
Lens Options		3-8mm, F1.4	7-22mm, F1.4
Horizontal Viewing Angle		96-38°	42-14°
Video			
Video Compression		H.264 Main/High Profile (MPEG-4 Part 10), triple-streaming	
Video Resolution		QHD (2560 x 1440)/Full HD 1080p/SXGA (1280 x 1024)/HD 720p/ XVGA/SVGA/D1/VGA/CIF/QVGA	
Video Streaming (Maximum Performance)		H.264 25/30 fps (PAL/NTSC) @ QHD or simultaneous QHD @ 12/15 fps + HD 720p @ 12/15 fps + D1 @ 12/15 fps (PAL/NTSC)	
Rate Control Option		CBR (64Kbps – 20,480Kbps), VBR	
Operation			
Image Setting	Brightness	Manual	
	Exposure	Auto iris, Auto/Fixed Shutter	
	Sharpness	Manual	
	Contrast	Manual	
	Hue	Manual	
	White Balance	Auto/Indoor/Outdoor/ATW/Manual	
	Gain (AGC)	Automatic	
	Backlight Compensation	On/Off	
	Digital Zoom	Supported (x2 to x10)	
	WDR	On/Off + 3 levels	
	3DNR	On/Off + 3 levels (with Latitude), On/Off + 6 levels (without Latitude)	
	Privacy Mask (Video Mask)	Web interface: On/Off. Up to five embedded web interfaces are supported in the streaming video output, but are not supported by Latitude. In the Latitude interface, the Privacy Mask is independent of the camera’s on-screen display and is not embedded.	
	IR Function	Day/Night (Auto/On/Off/Smart)	
Audio	Two-way Audio	Line out/Line in	
	Compression	G.711/G.726 (not supported by Latitude)	
Alarm	Input	1x 5V 10kΩ pull up dry contact	
	Output	1x Photo Relay Output 300V DC/AC @ 130mA maximum	
Signal-to-Noise Ratio		±50dB	
Event Notification		HTTP, FTP, SMTP	

Operation		
Languages		English, German, Spanish, French, Italian, Japanese, Korean, Portuguese, Russian, Simplified Chinese, and Traditional Chinese
Analytics		
Motion Detection		On/Off, plus sampling pixel interval, detection level, sensitivity level, and time interval settings.
Regions of Interest		Web interface: Configurable up to 10 ROI masks. Latitude interface: Configurable up to six ROI masks.
Motion Metadata		Streaming and recorded video includes per frame level motion metadata. Motion metadata is archive searchable by ROI via the Latitude Control Center user interface.
Triggered Actions		Notifications, On-Event Recording and Relay Output Command. Includes configurable alarms and broad range of recording on detection of video and snapshots.
Tampering Alarm		On/Off, plus duration, on-event notification, recording to SD card, recording to NAS, and more are supported as events in Latitude.
IR Illuminator		
Working Distance		40 meters (131 ft.) at 60°
Wavelength		850nm
IR Sensitivity		Yes (680-1100nm)
LEDs		6
Network		
Interface		10/100/1000Mbps Ethernet, Auto-sensing, Full/Half-Duplex
Protocols		IPv4/v6, TCP/IP, UDP, RTP, RTSP, HTTP, HTTPS, ICMP, FTP, SMTP, DHCP, PPPoE, UPnP, IGMP, SNMP,SNTP, QoS, IEEE 802.1X, ONVIF Version 2.4 Profile S
Password Levels		User and Administrator
Security		HTTPS, IP Filter, IEEE 802.1x
Firmware Upgrade		Flash memory for upgrade of camera firmware over the network (1GB Flash/8GB RAM)
Operating Systems		Windows XP, 7, 8, and 8.1
Internet Browser		Internet Explorer (IE 9, 10, and 11)
User Accounts		20
Mechanical		
Connectors	Power	3-pin terminal block
	Ethernet	RJ45
	Audio	1x Line-in and 1x Line-out 1.5mm audio jack
	Alarm	4-pin terminal block with 2-pin alarm input and 2-pin relay output
	Analog Video	1.0V p-p/75Ω, BNC (continuously enabled)
LED Indicator		Power, Link, ACT
Weatherproof Standard		IP66
Mechanical IR Cut Filter		Included
Bubble Rating		IK10 Vandal-Resistant Polycarbonate
Bubble F-Stop		Clear Bubble: F0.0, Smoke Bubble (optional): F1.0
Pan/Rotate/Tilt		355° pan, ±100° rotate, 80° tilt
MicroSDXC Card Recording		Up to 128GB, Class 10 (card not included)

Physical		
Dimensions (L x W)		164 x 104 mm (6.43 x 4.09 in.)
Weight		0.84 kg (1.86 lbs.)
Electrical		
Power Consumption	Indoor	6W
	Outdoor	13W with heater and IR
Power Source		12VDC (± 10%), 24VAC (± 10%), PoE (802.3af Class 0)
Environmental		
Operating Temperature		-40° to 50°C (-40° to 122°F) with heater -25°C to 50°C (-13° to 122°F) for cold start with POE
Humidity		10-95% non-condensing
General		
Regulatory	US	FCC 47 CFR Part 15, Subpart B, Class A; UL 60950
	Europe	CE (EN 55022-1998 Class A; EN 50130-4; EN 60950) RoHS
Warranty		Four-year limited warranty

A.2. CM-6208 Technical Specifications

Camera			
Image Sensor		1/1.7” 4072 x 3076 (12 MP) Progressive Scan BSI CMOS	
Effective Pixels		3840 x 2160 (H x V)	
Shutter Speed		1.0 to 1/10,000 (auto)	
Digital Slow Shutter (DSS)		1/1 to 1/25 or 1/30 with ≤ 32x sensitivity boost in day/night mode	
Sensitivity		0.3 Lux @F1.4 in color mode; 0.04 Lux @ F1.4 in night mode with IR illuminator ON, measured with DSS OFF at 30 IRE	
Enclosure		Tamper-resistant surface mount plastic case	
Lens		**CM-6208-11-I**	**CM-6208-21-I**
Lens Type		Varifocal Motorized F1.4 P-Iris with auto-focus and True Day/Night	
Lens Options		3.5-8mm	9-22mm
Horizontal Viewing Angle		116-50°	45-18°
Video			
Video Compression		H.264 and MJPEG	
Video Resolution		UHD 4K (3840 x 2160)/Full HD 1080p/SXGA (1280 x 1024)/HD 720p/ XVGA/SVGA/D1/VGA/CIF/QVGA	
Video Streaming (Maximum Performance)		H.264 25/30 fps (PAL/NTSC) @ 4K or simultaneous 4K @ 12/15 fps + Full HD 1080p @ 12/15 fps + HD 720p @ 12/15 fps + D1 @ 12/15 fps (PAL/NTSC)	
Rate Control Option		CBR (64Kbps – 20,480Kbps), VBR	
Operation			
Image Setting	Brightness	Manual	
	Exposure	Auto-iris, Auto/Fixed Shutter	
	Sharpness	Manual	
	Contrast	Manual	
	Hue	Manual	
	White Balance	Auto/Indoor/Outdoor/ATW/Manual	
	Gain (AGC)	Automatic	
	Backlight Compensation	On/Off	
	Digital Zoom	Supported (x2 to x10)	
	WDR	On/Off + 3 levels	
	3DNR	On/Off + 3 levels (with Latitude), On/Off + 6 levels (without Latitude)	
	Privacy Mask (Video Mask)	Web interface: On/Off. Up to five embedded web interfaces are supported in the streaming video output, but are not supported by Latitude. In the Latitude interface, the Privacy Mask is independent of the camera’s on-screen display and is not embedded.	
	IR Function	Day/Night (Auto/On/Off/Smart)	
Audio	Two-way Audio	Line out/Line in	
	Compression	G.711/G.726 (not supported by Latitude)	
Alarm	Input	1x 5V 10kΩ pull up dry contact	
	Output	1x Photo Relay Output 300V DC/AC @ 130mA maximum	
Signal-to-Noise Ratio		±50dB	
Event Notification		HTTP, FTP, SMTP	

Operation		
Languages		English, German, Spanish, French, Italian, Japanese, Korean, Portuguese, Russian, Simplified Chinese, and Traditional Chinese
Analytics		
Motion Detection		On/Off, plus sampling pixel interval, detection level, sensitivity level, and time interval settings.
Regions of Interest		Web interface: Configurable up to 10 ROI masks. Latitude interface: Configurable up to six ROI masks.
Motion Metadata		Streaming and recorded video includes per frame level motion metadata. Motion metadata is archive searchable by ROI via the Latitude Control Center user interface.
Triggered Actions		Notifications, On-Event Recording and Relay Output Command. Includes configurable alarms and broad range of recording on detection of video and snapshots.
Tampering Alarm		On/Off, plus duration, on-event notification, recording to SD card, recording to NAS, and more are supported as events in Latitude.
IR Illuminator		
Working Distance		40 meters (131 ft.) at 60°
Wavelength		850nm
LEDs		6
Network		
Interface		10/100/1000Mbps Ethernet, Auto-sensing, Full/Half-Duplex
Protocols		IPv4/v6, TCP/IP, UDP, RTP, RTSP, HTTP, HTTPS, ICMP, FTP, SMTP, DHCP, PPPoE, UPnP, IGMP, SNMP,SNTP, QoS, IEEE 802.1X, ONVIF Version 2.4 Profile S
Password Levels		User and Administrator
Security		HTTPS, IP Filter, IEEE 802.1x
Firmware Upgrade		Flash memory for upgrade of camera firmware over the network (1GB Flash/8GB RAM)
Operating Systems		Windows XP, 7, 8, and 8.1
Internet Browser		Internet Explorer (IE 9, 10, and 11)
User Accounts		20
Mechanical		
Connectors	Power	3-pin terminal block
	Ethernet	RJ45
	Audio	1x Line-in and 1x Line-out 1.5mm audio jack
	Alarm	4-pin terminal block with 2-pin alarm input and 2-pin relay output
	Analog Video	1.0V p-p/75Ω, BNC (continuously enabled)
LED Indicator		Power, Link, ACT
Weatherproof Standard		IP66
Mechanical IR Cut Filter		Included
Pan/Rotate/Tilt		355° pan, ±100° rotate, 80° tilt
MicroSDXC Card Recording		Up to 128GB, Class 10 microSDXC card (card not included)
Physical		
Dimensions (L x W)		218 x 99 mm (8.59 x 3.89 in.)
Weight		0.98 kg (34.5 oz.)

Electrical		
Power Consumption	Indoor	6W
	Outdoor	13W with heater and IR
Power Source		12VDC (± 10%), 24VAC (± 10%), PoE (802.3af Class 0)
Environmental		
Operating Temperature		-40° to 50°C (-40° to 122°F) with heater -25°C to 50°C (-13° to 122°F) for cold start with POE
Humidity		10-95% non-condensing
General		
Regulatory	US	FCC 47 CFR Part 15, Subpart B, Class A; UL 60950
	Europe	CE (EN 55022-1998 Class A; EN 50130-4; EN 60950) RoHS
Warranty		Four-year limited warranty

A.3. Internet Security Settings

If ActiveX control installation is blocked, either set Internet security level to default or change ActiveX controls and plug-in settings.

To set the default Internet security level

1. Start Internet Explorer (IE).
2. From the Command Bar toolbar, select Tools and select Internet Options from the menu that appears.

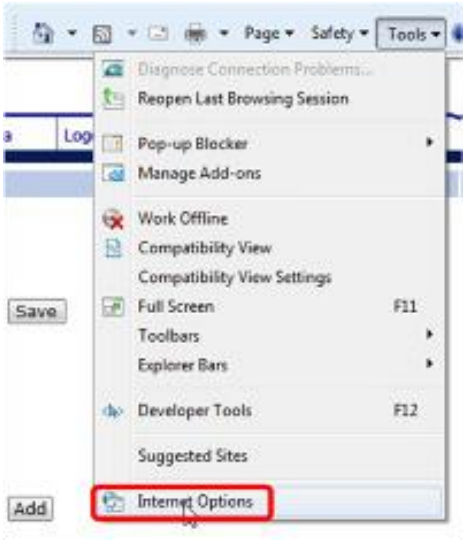


Figure 114: Command Bar Toolbar – Select Internet Options

3. In the Internet Options window that appears, select the Security tab.
4. Select

in Select a zone to view or change security settings.
5. If the settings are not defined as default, select Default Level and move the *Allowed* levels for this zone slider to *Medium-high* and select **OK**.

Figure 115: Internet Options Screen

6. Close all browsers and reopen so that the settings take effect.

ActiveX Controls and Plug-in Settings

To create a custom level

1. Start Internet Explorer (IE).
2. From the Command Bar toolbar, select **Tools** and select *Internet Options* from the menu that appears.

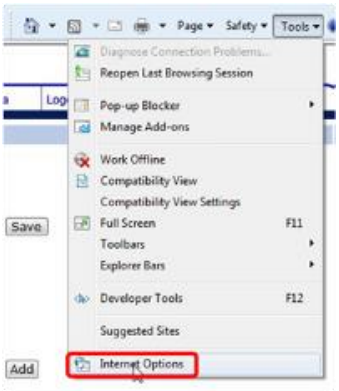


Figure 116: Command Bar Toolbar – Internet Options

3. In the **Internet Options** window that appears, select the **Security** tab.
4. If not already selected, select

, then select *Custom Level*.
5. In the dialog that appears, under **ActiveX controls and plug-ins** set ALL the following options (listed below) to **Enable** or **Prompt**:
   - Automatic prompting for ActiveX controls
   - Binary and script behaviors
   - Download signed ActiveX controls
   - Download using ActiveX controls
   - Initialize and script ActiveX not marked as safe
   - Run ActiveX controls and plug-ins
   - Script ActiveX controls marked safe for scripting

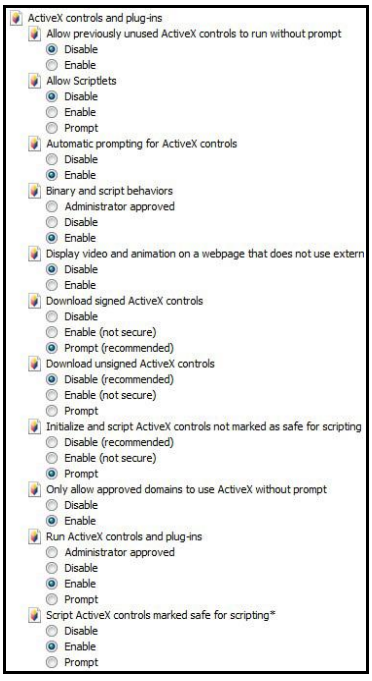
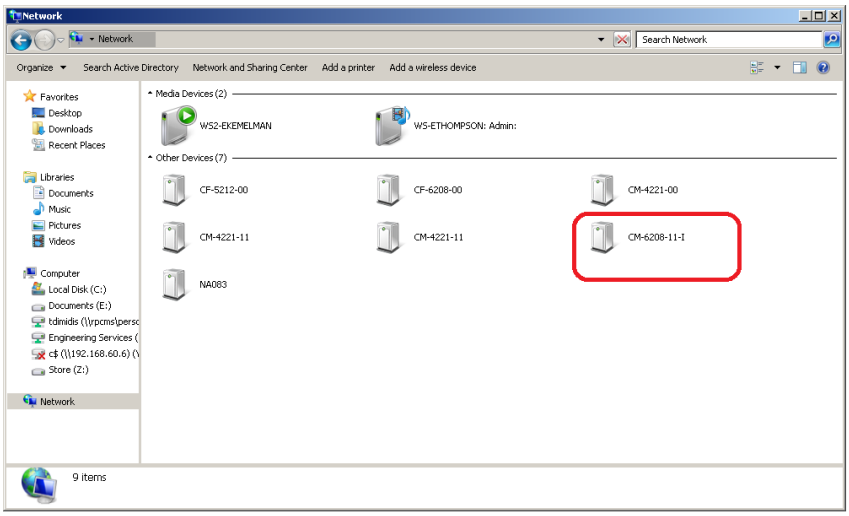


Figure 117: Schedule Screen

6. Click **OK** to accept the settings and close the **Security** screen.
7. Click **OK** to close the **Internet Options** screen.
8. Close the browser window and restart IE again to access the camera.

A.4. Install UPnP Components

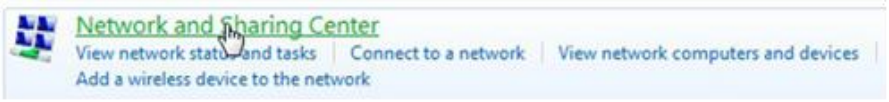
Follow the instructions below to enable UPnP so that the camera can be discovered and displayed in Network locations under *Other Devices*:



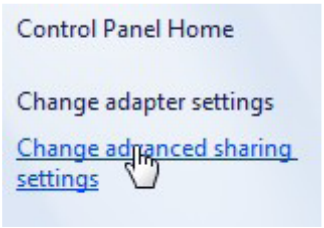
To enable UPnP discovery in Windows 7, 8, and 8.1

1. Click (Start) and select *Control Panel*.
2. Click *Network and Internet.*

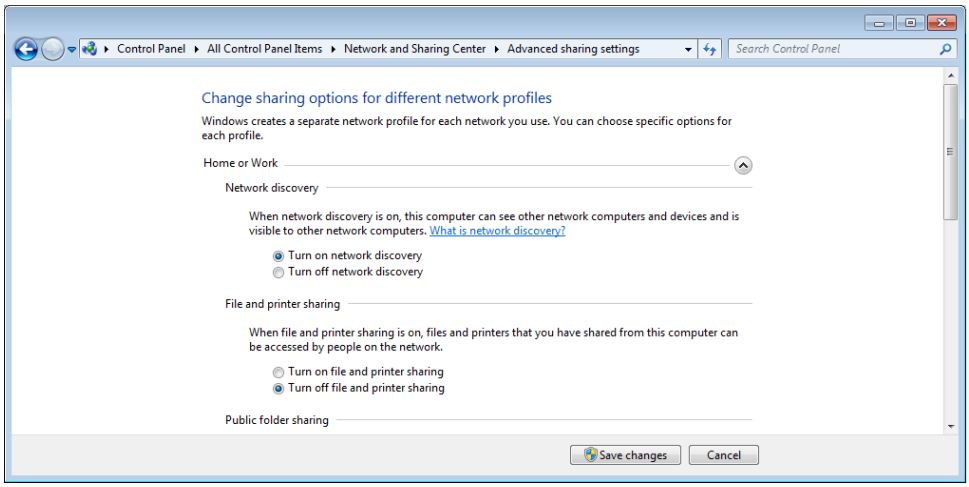
3. Click *Network and Sharing Center*.


Network and Sharing Center
View network status and tasks
Connect to a network
View network computers and devices
Add a wireless device to the network

4. Click *Change advanced sharing settings*.



5. Expand the Home or Work node, select *Turn on network discovery.*

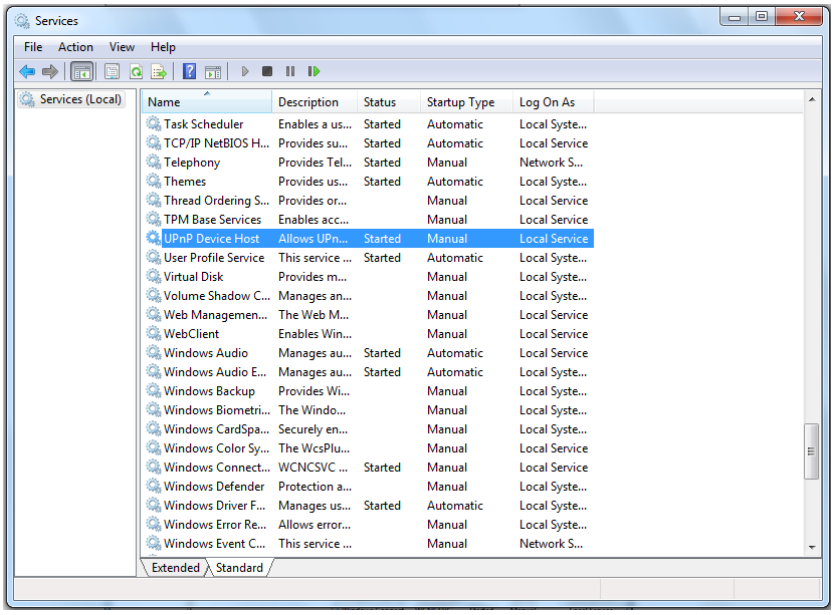

Control Panel ▸ All Control Panel Items ▸ Network and Sharing Center ▸ Advanced sharing settings
Search Control Panel
Change sharing options for different network profiles
Windows creates a separate network profile for each network you use. You can choose specific options for each profile.
Home or Work
Network discovery
When network discovery is on, this computer can see other network computers and devices and is visible to other network computers. What is network discovery?
Turn on network discovery
Turn off network discovery
File and printer sharing
When file and printer sharing is on, files and printers that you have shared from this computer can be accessed by people on the network.
Turn on file and printer sharing
Turn off file and printer sharing
Public folder sharing
Save changes
Cancel

6. Click **Save Changes**.

> **Note:**
> Network discovery requires that the DNS Client, Function Discovery Resource Publication, SSDP Discovery, and UPnP Device Host services are started, that network discovery is allowed to communicate through Windows Firewall, and that other firewalls are not interfering with network discovery.

To check that the UPnP Device Host services are running

1. Click (Start) and type in the Search programs and files field **services.msc** and then select **services.msc** from the displayed Programs. The **Services manager** dialog box appears.


Services
File Action View Help
Services (Local)
Name Description Status Startup Type Log On As
Task Scheduler Enables a us... Started Automatic Local Syste...
TCP/IP NetBIOS H... Provides su... Started Automatic Local Service
Telephony Provides Tel... Started Manual Network S...
Themes Provides us... Started Automatic Local Syste...
Thread Ordering S... Provides or... Manual Local Service
TPM Base Services Enables acc... Manual Local Service
UPnP Device Host Allows UPn... Started Manual Local Service
User Profile Service This service ... Started Automatic Local Syste...
Virtual Disk Provides m... Manual Local Syste...
Volume Shadow C... Manages an... Manual Local Syste...
Web Managemen... The Web M... Manual Local Service
WebClient Enables Win... Manual Local Service
Windows Audio Manages au... Started Automatic Local Service
Windows Audio E... Manages au... Started Automatic Local Syste...
Windows Backup Provides Wi... Manual Local Syste...
Windows Biometri... The Windo... Manual Local Syste...
Windows CardSpa... Securely en... Manual Local Syste...
Windows Color Sy... The WcsPlu... Manual Local Service
Windows Connect... WCNCSVC ... Started Manual Local Service
Windows Defender Protection a... Manual Local Syste...
Windows Driver F... Manages us... Started Automatic Local Syste...
Windows Error Re... Allows error... Manual Local Syste...
Windows Event C... This service ... Manual Network S...
Extended Standard

2. In the **Services manager** dialog box, scroll down the list to *UPnP Device Host* and verify that it shows the status *Started*. If *Started* is not displayed, right-click and select **Start** from the shortcut menu.

A.5. Deleting the Existing DVPlayer

Users who have previously installed the DVPlayer in the PC should first delete the existing DVPlayer from the PC before accessing the camera.

To delete a legacy DVPlayer

1. Click **Start** and select Control Panel.
2. In the Control Panel, click **Uninstall a program**.

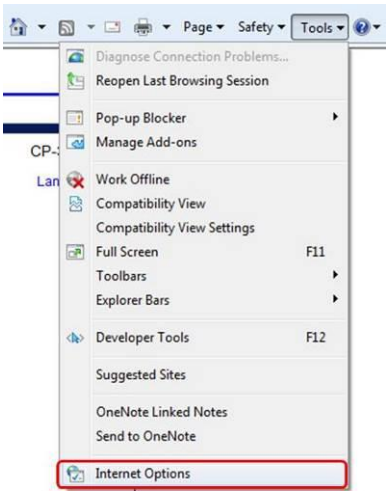
3. From the installed program list, select **DVPlayer** and then, on the banner bar, click **Uninstall**.
4. If prompted to confirm the Uninstall, click **Yes**.

A.6. Deleting Temporary Internet Files

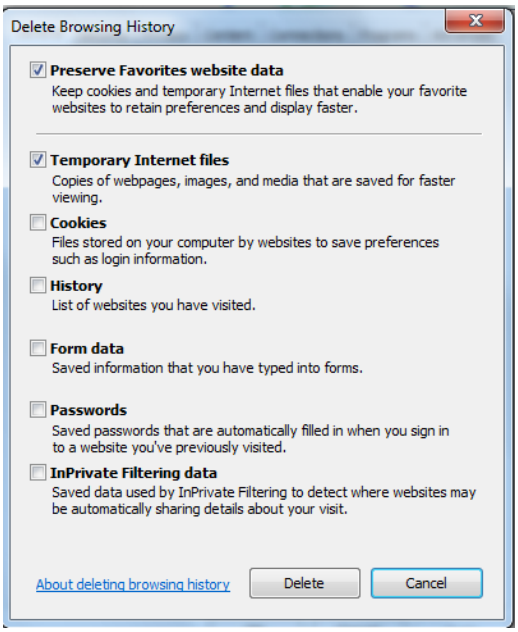
To improve browser performance, it is recommended to clean up all of the temporary Internet files.

To delete temporary Internet files

1. In Internet Explorer (IE), from the Command Bar toolbar, click **Tools** and select *Internet Options* from the menu that appears.



2. In the **General** tab in the *Internet Options* dialog box, click **Delete**.
3. In the **Delete Browser History** dialog box that appears, select Temporary Internet files. Deselect *Cookies and History* to keep this data. Then click **Delete**.


Delete Browsing History
Preserve Favorites website data
Keep cookies and temporary Internet files that enable your favorite websites to retain preferences and display faster.
Temporary Internet files
Copies of webpages, images, and media that are saved for faster viewing.
Cookies
Files stored on your computer by websites to save preferences such as login information.
History
List of websites you have visited.
Form data
Saved information that you have typed into forms.
Passwords
Saved passwords that are automatically filled in when you sign in to a website you've previously visited.
InPrivate Filtering data
Saved data used by InPrivate Filtering to detect where websites may be automatically sharing details about your visit.
About deleting browsing history
Delete
Cancel

A.7. Mounting Accessories

The following mounting accessories are available from DVTEL for installation of your Quasar Gen II CM-6204 Series Mini-Dome IP Camera. For more information on available options, contact your DVTEL sales representative or visit www.DVTEL.com to request details on where to get the accessories you need.

Image	Name	Description
	CM-CAPX-IND-W	Indoor wall mounting kit. Includes pendant cap with 18cm (7.1 in.) threaded wall mount bracket.
	CM-CAPX-IND-P	Indoor pendant mounting cap. Ready for ¾” conduit or 1-1/2” threaded mount.
	CM-CAPX-OUT-W	Outdoor wall mounting kit. Includes sunshield and pendant cap with 18cm (7.1 in.) threaded wall mount bracket.
	CM-CAPX-OUT-P	Outdoor pendant cap. Includes 1-1/2” male pipe threaded mount and ¾” female EMT conduit compatibility.
	CM-RCSD-62	Recessed mounting kit. Included peel and stick template, top-mounted 4S electrical box attachment points. For maximum surface thickness of 42mm (1-3/4”).
	CM-SMOKE-62	Smoked bubble cover. Full F-stop darkening of camera interior.
	CM-4S-62	4S electrical box mounting adapter. Rotates camera position by 45° when mounting to a 4S electrical box.
	CM-F150-62	1-1/2” threaded quarter-turn adapter.

Image	Name	Description
	CX-F125-0	1-1/4” inner threaded quarter-turn adapter.
	CX-F150-0	1-1/2” inner threaded quarter-turn adapter.
	CX-PLBX-0	Pole Mount Box. Includes CX-ARMX-1 Mounting Arm.

Contacting DVTEL

DVTEL Inc. is a multiple award-winning market leader in the development and delivery of intelligent security solutions over IP networks. DVTEL provides unified solutions that leverage existing network infrastructure, while providing unmatched levels of flexibility, scalability and cost-effectiveness - all backed by superior customer support.

To contact us, write us at info@DVTEL.com, or contact your local office.

CORPORATE HEADQUARTERS **DVTEL, Inc.** 65 Challenger Road Ridgefield Park, NJ 07660 USA Tel: +1 201.368.9700 Fax: +1 201.368.2612 info@DVTEL.com	**ASIA PACIFIC REGION** **DVTEL** 111 North Bridge Road, #27-01 Peninsula Plaza Singapore 179098 Tel: +65 6389 1812 Fax: +65 6491 5660 info.apac@DVTEL.com
ANZ AND THE PACIFIC ISLANDS **DVTEL** 37 Victoria Street Henley Beach, SA 5022 Australia Tel: +61 8 8235 9211 Fax: +61 8 8235 9255 info.anz@DVTEL.com	**EMEA** **DVTEL UK Ltd.** 7 Lancaster Court Coronation Road High Wycombe HP12 3TD England Tel: +44 (0) 1494 412240 Fax: +44 (0) 1494 446928 info.uk@DVTEL.com
INDIA AND SAARC, GULF REGION **DVTEL, India Pvt., Ltd** 123 SSR Corporate Park Mathura Road Faridabad 121002 Haryana, India Tel: +91 (129) 431 5031 Fax: +91 (129) 431 5033 info.asia@DVTEL.com	**CENTRAL AND LATIN AMERICA** **DVTEL Mexico S.A.P.I. de C.V**. Felipe Villanueva No. 10 Col. Guadalupe Inn México D. F. 01020 México Tel: +52 55 5580 5618 Fax: +52 55 8503 4299 info.cala@DVTEL.com
DVTEL NORTH ASIA 2404, 24/F, World-Wide House 19 Des Voeux Road Central Hong Kong Tel: +852 3667 9295 Mobile: +852 9479 4195 info.northasia@DVTEL.com	**DVTEL 中国** **北京朝阳区西大望路甲1号 温特莱中心B座12层09** 单元 100026 电话: +86-10-8586-8836 **手机**: +86-13501266857 传真: +86-10-8586-8812 邮箱: info.china@DVTEL.com

To request the latest versions of firmware and software or to download other product-related documents, visit http://www.DVTEL.com/support. If you have obtained a login, go to our support gateway. For assistance, email us at support@DVTEL.com or phone 1-888-DVTEL77.